Kaspersky Security 8.0 for Microsoft SharePoint Server

Administrator's Guide

APPLICATION VERSION: 8.0

Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers regarding this software product.

Warning! This document is the property of Kaspersky Lab: All rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability by applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

Kaspersky Lab reserves the right to amend this document without additional notification. The latest version of this document can be found on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document the rights to which are held by third parties, or for any potential damages associated with the use of such documents.

Document revision date: 10/17/2013

http://www.kaspersky.com
http://support.kaspersky.com

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document is the Administrator's Guide to Kaspersky Security 8.0 for Microsoft SharePoint Server® (hereafter "Kaspersky Security" or "application").

This Guide is intended for technical specialists tasked with installing and administering Kaspersky Security and supporting companies that use Kaspersky Security.

This Guide is intended to do the following:

- Help you install, activate, and use Kaspersky Security.
- Provide advice on Kaspersky Security support and administration after installation.
- Provide a readily search able source of information for questions related to operation of Kaspersky Security.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

IN THIS DOCUMENT

This document includes the following sections:

Sources of information about the application (see page 10)

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

Kaspersky Security 8.0 (see page 12)

This section describes the features of the application and provides brief information about application functions and components. You will find out what the distribution kit includes and which services are available to registered users of the application. The section provides information about the hardware and software requirements that a computer must meet to support installation.

Application interface (see page 18)

This section describes the basic elements of the graphical user interface of the application: the main window, Administration Console, the Administration Console tree, and the details pane.

Server protection status (see page 20)

This section describes how you can check the level of server protection using Administration Console: to view license info, the status of application modules, as well as statistics on the number of objects scanned and threats detected.

Application licensing (see page 26)

This section provides information about general terms related to the application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.

Getting started (see page 31)

This section explains how to begin using Kaspersky Security and connect Administration Console to one or several SharePoint servers.

Updating databases (see page 33)

This section explains how to update application databases and configure database updates.

On-access scanning (see page 38)

This section describes the process of scanning objects as they are uploaded to a SharePoint server and downloaded to the user's computer from the server, and contains instructions on configuring the scan settings.

On-demand scanning (see page 50)

This section describes the process of scanning of objects hosted by a SharePoint server and configuring scan settings.

Content filtering (see page 62)

This section describes the process of scanning web objects for unwanted content, malicious or phishing URLs and instructions for configuring scan settings.

Backup (see page 72)

This section contains information about Backup and how to use it.

Notifications (see page 84)

This section describes how you can configure notifications about licensing events, system events, and application component events.

Reports (see page 87)

This section describes application activity reports, and contains guidelines on how to configure report schedules and report generation settings.

Configuring application settings (see page 94)

This section contains information about advanced application settings and how to configure them.

Contacting Technical Support (see page 99)

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

Glossary (see page 102)

This section contains a list of terms mentioned in the document and their respective definitions.

Kaspersky Lab ZAO (see page 105)

This section provides information about Kaspersky Lab ZAO.

Information about third-party code (see page 106)

This section provides information about the third-party code used in the application.

Trademark notices (see page 107)

This section lists trademarks of third-party manufacturers that were used in the document.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
It is recommended to use...	Notes are boxed. Notes may contain useful tips, advice, specific values of settings or important particular cases in the operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of application statuses and events.
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➨ *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
Enter help in the command line The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION:

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- Application page on the Kaspersky Lab website
- Application page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 99).

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On the web page (http://www.kaspersky.com/products/business/applications/security-sharepoint), you can view general information about the application, its functions, and its features.

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with Kaspersky Lab applications. Knowledge Base comprises reference articles that are grouped by topic.

On the page of the application in the Knowledge Base (http://support.kaspersky.com/sharepoint), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles may provide answers to questions that are out of scope of Kaspersky Security, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

Online help

The online help of the application comprises help files.

Online help contains information about each window of the application: the list of settings, their descriptions and links to the tasks using these settings.

Full help provides information about managing computer protection, configuring the application and solving typical user tasks.

Documentation

The package of application manuals includes the following documents: *Installation Guide for Kaspersky Security 8.0 for SharePoint Server* and *Administrator's Guide to Kaspersky Security 8.0 for SharePoint Server* (this Guide). These manuals will help you to install and activate the application on local area network computers, configure application settings, and find tips on using the application.

The latest versions of the manuals are available on the update download page (http://www.kaspersky.com/product-updates/sharepoint-security).

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum (http://forum.kaspersky.com/index.php?showforum=5).

In this forum you can view existing topics, leave your comments, create new topics.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our HQ office in Moscow by phone (http://www.kaspersky.com/contacts).
- By emailing your question to sales@kaspersky.com.

The service is provided in Russian and English.

CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT

To contact the Technical Writing and Localization Unit, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Security 8.0 for SharePoint Server" as the subject line in your message.

KASPERSKY SECURITY 8.0 FOR SHAREPOINT SERVER

Kaspersky Security is an application for protection of servers running Microsoft® SharePoint Server against malicious objects and unwanted content.

Kaspersky Security can perform the following operations:

- Scan files and web objects hosted by SharePoint servers as they are uploaded to the server or downloaded from the server to the user's computer.
- Scan files and web objects hosted by SharePoint servers manually or schedule an automatic scan.
- Configure the scanning of SharePoint web objects: create custom scan categories, specify the type and format of unwanted files, and create masks of unwanted file names.
- Configure application actions on files containing malicious objects and web objects containing unwanted content or malicious and phishing URLs.
- Specify areas in the tree of SharePoint server nodes that need scanning, and exclude certain areas from the scan scope to ease the load on the server.
- Use Kaspersky Security Network to increase the effectiveness of protection of SharePoint servers.
- Scan files for malicious code that exploits system vulnerabilities.
- Save copies of the documents in Backup before disinfecting or deleting them.
- Generate reports on the results of scanning of files and SharePoint web objects manually or automatically according to schedule.

IN THIS SECTION:

DISTRIBUTION KIT

You can purchase the application through Kaspersky Lab's online stores (for example, http://www.kaspersky.com, in the **eStore** section) or partner companies.

Kaspersky Security is supplied as part of the applications Kaspersky Security for collaboration servers (http://www.kaspersky.com/business-security/collaboration) and Kaspersky Total Security (http://www.kaspersky.com/business-security/total).

After buying a license for Kaspersky Security, you will receive an email with a link for downloading the application from the eStore website along with an application key file, or a CD with the distribution kit containing the application files and manuals.

Carefully review the End User License Agreement between installing and using the application.

For more details on ways of purchasing and the distribution kit, contact the Sales Department by sending a message to sales@kaspersky.com.

SERVICE FOR USERS

By purchasing a license for the application, you can benefit from the following services during the entire term of the license:

- Database updates and new versions of the application
- Advice on issues related to the installation, configuration and use of the application by phone or via email
- Announcements of new Kaspersky Lab releases and information about new viruses and outbreaks To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support website.

> Advice on issues related to operating systems and third-party applications and technologies is not provided.

HARDWARE AND SOFTWARE REQUIREMENTS

To ensure the application runs smoothly, the computer must meet the following minimum hardware and software requirements.

Hardware requirements

For SharePoint Server 2007:

- If installing Administration Console and Security Server:
  - Minimum 2.5 GHz processor (two 3 GHz processors or higher recommended)
  - 1 GB RAM (2 GB recommended)
  - 229 MB of available disk space
- If installing only Administration Console:
  - Minimum 400 MHz processor (1 GHz recommended)
  - 256 MB RAM
  - 176 MB of available disk space

For SharePoint Server 2010:

- If installing Administration Console and Security Server:
  - 64-bit quad-core processor
  - 4 GB RAM
  - 229 MB of available disk space
- If installing only Administration Console:
  - Minimum 400 MHz processor (1 GHz recommended)

  - 256 MB RAM
  - 176 MB of available disk space

For SharePoint Server 2013:

- If installing Administration Console and Security Server:
  - 64-bit quad-core processor
  - 8 GB RAM
  - 229 MB of available disk space
- If installing only Administration Console:
  - Minimum 400 MHz processor (1 GHz recommended)
  - 256 MB RAM
  - 176 MB of available disk space

> Depending upon the application settings and its mode of operation, more disk space may be required for Backup and other service folders.

Software requirements

Required components to install the application:

- Microsoft SharePoint Server 2007, Microsoft SharePoint Server 2010 or Microsoft SharePoint 2013

  > Standalone installation of Administration Console does not require Microsoft SharePoint Server

- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft Management Console 3.0

Supported versions of SharePoint servers:

- Microsoft SharePoint Server 2007
- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013

Supported operating systems:

For SharePoint Server 2007 x86 / x64:

- If installing Administration Console and Security Server:
  - Windows Server® 2003
  - Windows Server 2003 x64
  - Windows Server 2003 R2

  - Windows Server 2003 R2 x64
  - Windows Server 2008
  - Windows Server 2008 x64
  - Windows Server 2008 R2
  - Windows Server 2012 R2
- If installing only Administration Console:
  - Windows Server 2003
  - Windows Server 2003 x64
  - Windows Server 2003 R2
  - Windows Server 2003 R2 x64
  - Windows Server 2008
  - Windows Server 2008 x64
  - Windows Server 2008 R2
  - Windows Server 2012 x64
  - Windows Server 2012 R2
  - Microsoft Windows® XP x64 Service Pack 2
  - Microsoft Windows XP Service Pack 3
  - Microsoft Windows Vista® Service Pack 2
  - Microsoft Windows Vista x64 Service Pack 2
  - Windows 7 Professional Service Pack 1
  - Windows 7 Professional x64 Service Pack 1
  - Windows 7 Enterprise Service Pack 1
  - Windows 7 Enterprise x64 Service Pack 1
  - Windows 7 Ultimate Service Pack 1
  - Windows 7 Ultimate x 64 Service Pack 1
  - Windows 8
  - Windows 8 x64
  - Windows 8.1

For SharePoint Server 2010:

- If installing Administration Console and Security Server:
  - Windows Server 2008 x64

    - Windows Server 2008 R2
    - Windows Server 2012 R2
- If installing only Administration Console:
    - Windows Server 2003
    - Windows Server 2003 x64
    - Windows Server 2003 R2
    - Windows Server 2003 R2 x64
    - Windows Server 2008
    - Windows Server 2008 x64
    - Windows Server 2008 R2
    - Windows Server 2012 x64
    - Windows Server 2012 R2
    - Microsoft Windows XP x64 Service Pack 2
    - Microsoft Windows XP Service Pack 3
    - Microsoft Windows Vista Service Pack 2
    - Microsoft Windows Vista x64 Service Pack 2
    - Windows 7 Professional Service Pack 1
    - Windows 7 Professional x64 Service Pack 1
    - Windows 7 Enterprise Service Pack 1
    - Windows 7 Enterprise x64 Service Pack 1
    - Windows 7 Ultimate Service Pack 1
    - Windows 7 Ultimate x 64 Service Pack 1
    - Windows 8
    - Windows 8 x64
    - Windows 8.1

For SharePoint Server 2013:

- If installing Administration Console and Security Server:
    - Windows Server 2008 R2 x64 Service Pack 1
    - Windows Server 2012 x64
    - Windows Server 2012 R2
- If installing only Administration Console:

- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2003 R2
- Windows Server 2003 R2 x64
- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012 x64
- Windows Server 2012 R2
- Microsoft Windows XP x64 Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows Vista Service Pack 2
- Microsoft Windows Vista x64 Service Pack 2
- Windows 7 Professional Service Pack 1
- Windows 7 Professional x64 Service Pack 1
- Windows 7 Enterprise Service Pack 1
- Windows 7 Enterprise x64 Service Pack 1
- Windows 7 Ultimate Service Pack 1
- Windows 7 Ultimate x 64 Service Pack 1
- Windows 8
- Windows 8 x64
- Windows 8.1

Supported browsers:

- Windows Internet Explorer® 7.x (32-bit version)
- Windows Internet Explorer 7.x (64-bit version)
- Windows Internet Explorer 8.x (32-bit version)
- Windows Internet Explorer 8.x (64-bit version)
- Windows Internet Explorer 9.x (32-bit version)
- Windows Internet Explorer 9.x (64-bit version)
- Mozilla™ Firefox™ 3.6
- Google Chrome™ (last version)

APPLICATION INTERFACE

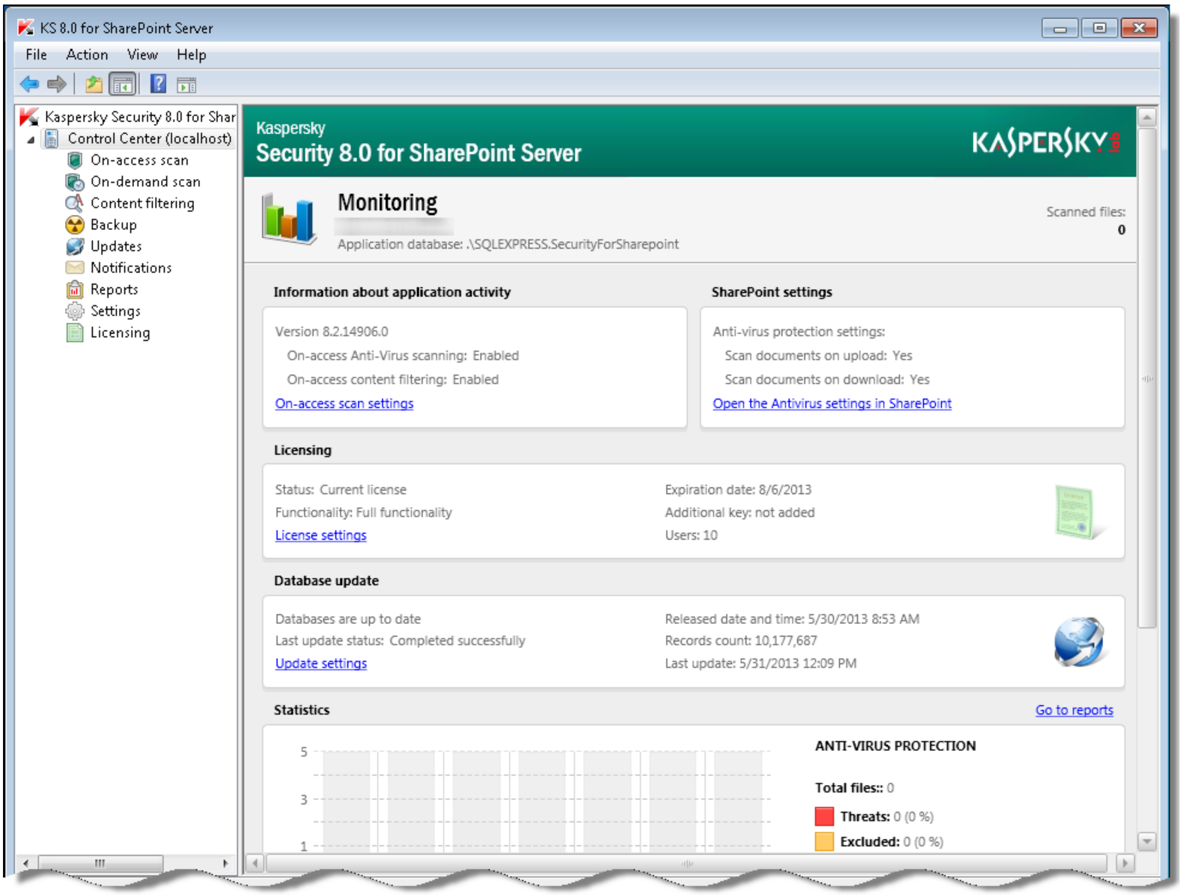
This section describes the basic elements of the graphical user interface of the application: the main window, Administration Console, the Administration Console tree, and the details pane.

IN THIS SECTION:

MAIN WINDOW

Interaction with the application takes place via Administration Console. Administration Console is a standalone independent snap-in for Microsoft Management Console (MMC).

Main window of Administration Console consists of the following parts (see the figure below):



Application database: .\SQLEXPRESS.SecurityForSharepoint

Scanned files: 0

Information about application activity

Version 8.2.14906.0

On-access Anti-Virus scanning: Enabled

On-access content filtering: Enabled

On-access scan settings

SharePoint settings

Anti-virus protection settings:

Scan documents on upload: Yes

Scan documents on download: Yes

Open the Antivirus settings in SharePoint

Licensing

Status: Current license

Functionality: Full functionality

License settings

Expiration date: 8/6/2013

Additional key: not added

Users: 10

Database update

Databases are up to date

Last update status: Completed successfully

Update settings

Released date and time: 5/30/2013 8:53 AM

Records count: 10,177,687

Last update: 5/31/2013 12:09 PM

Statistics

Go to reports

ANTI-VIRUS PROTECTION

Total files:: 0

🟥 Threats: 0 (0 %)

🟧 Excluded: 0 (0 %)

Figure 1: Main window of Administration Console

- **Toolbar**. Displayed in the upper part of the main window. It contains a set of buttons providing direct access to some frequently used functions of the application.

- **Menu**. Located in the upper part of the main window above the toolbar. The menu provides management functions for files and windows, as well as access to the help system.

- **Administration Console tree**. It is located in the left part of the main window. The Administration Console tree is used to view the list of SharePoint servers connected to Administration Console and manage the settings of the application installed on SharePoint servers. Connected servers and the settings of Kaspersky Security are listed as nodes.

- **Details pane**. It is located in the right part of the main window. It lets you view and configure application settings.

ADMINISTRATION CONSOLE TREE

The Administration Console tree shows the structure of profiles, SharePoint servers, and subnodes for managing application functions.

The topmost node of the console tree is **Kaspersky Security 8.0 for SharePoint Server**. Double-clicking it in the console tree with the mouse opens the list of connected to Administration Console SharePoint servers running installed Kaspersky Security.

Clicking the plus sign next to a connected server opens in the console tree the list of nested nodes designed for managing application functions. The list contains the following nodes:

- **On-access scan** – view and configure the settings of tasks that scan objects as they are uploaded to the server or downloaded to user workstations.

- **On-demand scan** – view and configure the settings of tasks that scan objects on the SharePoint server.

- **Content filtering** – view and configure the settings of tasks that scan the content of SharePoint web objects.

- **Backup** – view the contents of Backup.

- **Updates** – view and configure the settings of Anti-Virus and Content filtering category updates.

- **Notifications** – view and configure the settings of notifications about application events.

- **Reports** – view and configure the settings of Anti-Virus and Content filtering reports.

- **Settings** – view and configure advanced application settings: Kaspersky Security Network usage, email notifications, event logging, and Backup purging.

- **Licensing** – view information about added keys and manage keys.

DETAILS PANE

The details pane shows information about the current SharePoint server protection status, Kaspersky Security and application settings.

The appearance of the details pane depends on the node selected in the Administration Console tree.

SERVER PROTECTION STATUS

This section describes how you can check the level of server protection using Administration Console: to view license info, the status of application modules, as well as statistics on the number of objects processed and threats detected.

This section also covers the default settings of Kaspersky Security.

IN THIS SECTION:

DEFAULT PROTECTION

SharePoint protection against malware is enabled as soon as Kaspersky Security is installed and depends on the settings configured in the Application Configuration Wizard (*see the Installation Guide for Kaspersky Security 8.0 for SharePoint Server)*.

If anti-virus protection is enabled in the Application Configuration Wizard window, the following application mode is engaged:

- The application scans SharePoint web objects for viruses as they are uploaded to the server or downloaded from the server to the user's computer.
  - On detecting an infected or probably infected object on a SharePoint server, the application attempts to disinfect it.
  - On detecting a password-protected or corrupted web object, the application skips it and continues the scan.
- The application scans web objects for malware that exploits system vulnerabilities.
- The application does not scan web objects for unwanted content.

If the KSN agreement was accepted and the Kaspersky Security Network service enabled in the window of the Application Configuration Wizard, the application uses KSN information to protect the computer.

If all functions were disabled in the Application Configuration Wizard during installation, the application does not scan web objects as soon as it has been started.

VIEWING SHAREPOINT SERVER PROTECTION STATUS DETAILS

➧ *To view SharePoint server protection status details:*

1. Start Administration Console.

2. In the Administration Console tree, select the node corresponding to the SharePoint server whose protection status details you want to view.

   The details pane of the selected node corresponding to the SharePoint server displays the following tabs with protection status information:

   - **Events and statistics**.

   - **List of farm servers**.

   If Kaspersky Security is installed on a standalone server, the **List of farm servers** tab is not displayed.

   The **Events and statistics** tab contains information about the status of application components distributed across the following sections:

   - **Information about application activity** (see page 21).

   - **SharePoint settings** (see page 22).

   - **Licensing** (see page 22).

   - **Database update** (see page 23).

   - **Protection of farm servers** (see page 23).

   - **Statistics** (see page 24).

   The **List of farm servers** tab displays a table with information about the protection and update status of Kaspersky Security databases on all SharePoint farm servers. The table contains the following information:

   - Server name.

   - Protection status (see page 24).

   - Last update status (see page 25).

INFORMATION ABOUT APPLICATION ACTIVITY

The **Information about application activity** section shows the application version and status of its components. Available values:

- *Enabled*. Anti-Virus protection / Content filtering is enabled in the On-access scan node of Administration Console and is working correctly on all SharePoint farm servers.

- *Disabled*. Anti-Virus protection / Content filtering is disabled on all SharePoint farm servers.

- *Protection errors*. Errors detected in the operation of Anti-Virus protection / Content filtering on at least one of the SharePoint farm servers.

- *Unknown*. The status of anti-virus protection / Content filtering on at least one of the SharePoint farm servers is unknown.

The section contains a description of any errors that occur.

SHAREPOINT SETTINGS

This section displays information about the scan settings configured on the SharePoint server (see section "Kaspersky Security operation depending upon the SharePoint server settings" on page 40). If anti-virus protection is disabled on the SharePoint server, Kaspersky Security does not perform on-access anti-virus scanning or Content filtering.

LICENSING

The **Licensing** section shows general information about the current license and application functionality depending on the type of license purchased.

The **Key status** contains details of the active key. Available field values:

- *Valid license*. A key has been added, and the license has not expired.
- Errors on some farm servers. Licensing errors or violations have been detected on at least one of the SharePoint farm servers (for example, a key is missing or blacklisted). The error description is displayed in red, and the section itself is highlighted in orange.
- *None.* No key has been added, and Administration Console is deployed on a standalone SharePoint server.

The **Expiration date** field displays the expiration date of the license validity period.

If the number of days remaining on the license is less than the number of days specified in the **Notifications** node, the expiration date in the field is displayed in red. You are advised to add an additional key in the **Licensing** node before the current license expires.

The **Additional key** field contains information about the availability of an additional key. Available values:

- **Added**. An additional key has been added, and the validity period of the active key has not expired yet.
- **Not added**. One of two possibilities:
  - an additional key is not added;
  - an additional key is installed, but the active key has expired.

The **Users** field contains information about the maximum number of employees at the organization with access to a server protected by the application, in accordance with the End User License Agreement.

If Kaspersky Security is installed on a standalone server, the **Licensing** section displays the **Functionality** field with information about the functionality of the application. Available field values:

- **Full functionality**. No limitations apply to the operation of Kaspersky Security.
- **The license has expired. Database updates and technical support are unavailable**. Anti-Virus scanning and Content filtering are performed using the databases downloaded during the most recent update. To download the latest databases, you have to replace the key (see section "Replacing a key" on page 29).
- **Management only.** No key is installed, or the trial license has expired. Only management of Kaspersky Security is available. Anti-Virus scanning and Content filtering are not performed, and updates are not available.

- **Update only**. The key is in the black list. Only database updates are available. Anti-Virus scanning and Content filtering are not performed.

DATABASE UPDATE

The **Database update** section shows information about the current state of Anti-Virus databases, the date of the last update, and the number of records in databases.

The **Status** field displays information about the status of databases currently in use by Kaspersky Security.

If Kaspersky Security is installed on the SharePoint farm, the **Status** field can take the following values:

- *Databases are up to date on all farm servers*. Databases used on all SharePoint farm servers were updated in the past 24 hours and are not corrupted.
- *Databases on some farm servers are out of date*. Databases were not updated in the past 24 hours.
- *Databases on some farm servers are corrupted*. Databases are missing or corrupted, and cannot be read by the application on at least one SharePoint farm server.

If Kaspersky Security is installed on a standalone SharePoint server, the **Status** field can take the following values:

- *Databases are up to date*. Databases were updated in the past 24 hours and are not corrupted.
- *Update required*. Databases were not updated in the past 24 hours.
- *Databases corrupted*. Databases are missing or corrupted and cannot be read by the application.

The **Result of the last update** field displays the date and result of the most recent database update. If an error occurred during the last database update, the field contains a description of the error. In this case, the **Database update** section is highlighted orange, and the description of the error is displayed in red.

If Kaspersky Security is installed on a standalone SharePoint server, the section displays the **Last update** field, which contains the date and time of the most recent attempt to update the databases.

The **Release date and time** field shows the release date of the earliest database on all SharePoint farm servers. If the databases are out of date, the date is displayed in red. In this case, it is recommended that you go to the **Updates** node and update the databases.

The **Records count** field contains information about the total number of records in the databases on the server since the time of the first update.

PROTECTION OF SHAREPOINT FARM SERVERS

The **Protection of farm servers** section displays information about the current protection status of the SharePoint farm servers.

SharePoint farm servers that have not accessed the database within the past 60 seconds are considered inactive by the application. The number and list of such servers are shown in this section. Detailed information about why the database was not accessed is displayed in the table on the **Farm servers** tab.

If Kaspersky Security is installed on a standalone SharePoint server, the **Protection of farm servers** section is not displayed in the details pane of the **Control Center (<Server name>)** node.

STATISTICS

This section contains statistics on the operation of the application for the past week. The graph presents the following information about the number of positives returned by application components, the number of threats detected, files blocked, and clean files:

- **Anti-Virus protection**:
  - **Total files**. The total number of files that are infected, probably infected, corrupted, password-protected, or clean, and files that returned an error during Anti-Virus scanning.
  - **Threats**. The number of malicious objects detected in scanned files.
  - **Excluded**. The number of files excluded from the scan scope.
  - **Not infected.** The number of files scanned by the application and recognized as not infected.
  - **Other**. Files that do not match any other categories. The group includes, for example, files not scanned because of key errors or files that have caused errors while being processed.
- **Content filtering**:
  - **Total**. The total number of files and SharePoint web objects that caused Content filtering incidents (by content, by file type and format, and masks of unwanted file names), files with *Not infected* status, and files that returned Content filtering errors.
  - **Files with unwanted content**. Number of files that have been found by Content filtering to contain unwanted words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the Content filtering settings (see section "Configuring Content filtering" on page 57).
  - **Web objects with unwanted content**. The number of SharePoint web objects that have been found by Content filtering to contain unwanted words or phrases included in Kaspersky Lab sections and user categories, and the number of web objects found to contain malicious or phishing URLs.
  - **Files in unwanted formats**. Number of files in unwanted formats.
  - **Recognized as clean**. The number of files that are free from unwanted content (with the names and formats not matching the specified masks of unwanted file names and formats), malicious or phishing URLs.
  - **Other**. Files that do not match any other category including files unprocessed because of errors.

SHAREPOINT SERVER PROTECTION STATUS

The **Protection status** column in the **List of farm servers** table displays information about the current operational status of the Anti-Virus and Content filtering components during on-access scanning on the SharePoint server. Available values:

- **Protection is enabled**. Anti-virus scan / or Content filtering is enabled in the **On-access scan** node of Administration Console, and is working correctly on the SharePoint server.
- **Anti-virus scan / Content filtering is disabled**. Anti-virus scan and / or Content filtering is disabled in the **On-access scan** node.
- **Protection status unknown**. An outdated version of Kaspersky Security is installed on the SharePoint server, or the SharePoint server is unavailable.
- **Anti-Virus and /or Content filtering scan errors**. Anti-virus scan and / or Content filtering is enabled in the **On-access scan** node, but documents cannot be scanned due to license or database-related errors or other

errors in the operation of Kaspersky Security. In this case, the **Protection status** column contains information about the error.

DATABASE UPDATE STATUS

The **Status of the last update** column in the **List of farm servers** table displays information about the status of the last update of the Kaspersky Security databases on the server.

Available values:

- *Databases are up to date. Update is not required*. The most recent update was successful. Databases were updated in the past 24 hours and are not corrupted.
- *Databases are out of date. Update required*. Databases were not updated in the past 24 hours.
- *Databases corrupted. Update required*. Database files are missing or corrupted and cannot be read by the application.
- *Database update error*. The last database update attempt ended in an error. The column also contains the error description.

APPLICATION LICENSING

This section provides information about general terms related to the application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.

IN THIS SECTION:

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

Read through the terms of the License Agreement carefully before you start using the application.

It is deemed that you accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the End User License Agreement, you must abort the installation or do not use the application.

ABOUT THE LICENSE

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A current license entitles you to the following kinds of services:

- The right to use the application on one or several devices.
- Assistance from Kaspersky Lab Technical Support.
- Other services available from Kaspersky Lab or its partners during the term of the license (see the section "Service for users" on page 13).

The scope of services and application usage term depend on the type of license under which the application is activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

  Trial license usually has a short validity period. As soon as the trial license expires, all Kaspersky Security features are disabled. To continue using the application, you should purchase a commercial license.

- *Commercial* – a paid license offered upon purchase of the application.

When the commercial license expires, the application continues to work in limited functionality mode. You can still scan files for viruses and use other application components, but only with databases that are installed before the expiration of the license. To continue using all the functionality of Kaspersky Security, you have to renew the commercial license.

To ensure maximum protection, you are advised to renew your license before its expiry date.

ABOUT THE KEY FILE

A *key file* – is a file of the form xxxxxxxx.key. You are provided with a key file when you purchase the application. You may use the application only when you have a key file.

If the key file is accidentally deleted, you should send a request to Technical Support (see section "Contacting Technical Support" on page 99).

A key file contains the following data:

- Key – a unique alphanumeric sequence. A key is used, for example, to receive technical support from Kaspersky Lab.
- Employees number restriction - the maximum number of employees which have access to the server protected by the program.
- Name of user representative – the name of the contact person at the organization that purchased Kaspersky Security.
- License term is the period of software use specified in the License Certificate.

ABOUT DATA SUBMISSION

If you agree to participate in the Kaspersky Security Network (see section "Participating in the Kaspersky Security Network (KSN)" on page 94), the following information collected during the operation of Kaspersky Security on the computer is automatically forwarded to Kaspersky Lab:

- Application type
- Full application version
- Application installation ID
- Operating system version
- Operating system service pack version
- IP address of the SharePoint server hosting Kaspersky Security
- URL or IP address (IPv4 and IPv6 versions supported) of the phishing / malicious URL
- Anti-Virus database release date and time

Kaspersky Lab protects any information received in this way as prescribed by law. Kaspersky Lab uses any collected information as general statistics only. General statistics are automatically generated using original collected information and do not contain any private data or other confidential information. Original collected information is stored in encrypted form and destroyed as it is accumulated (twice per year). General statistics are stored indefinitely.

Participation in Kaspersky Security Network is voluntary. You can opt out of participating in Kaspersky Security Network at any time (see section "Configuring KSN protection settings" on page 95). No personal data of the user is collected, processed, or stored.

MANAGING KEYS IN KASPERSKY SECURITY

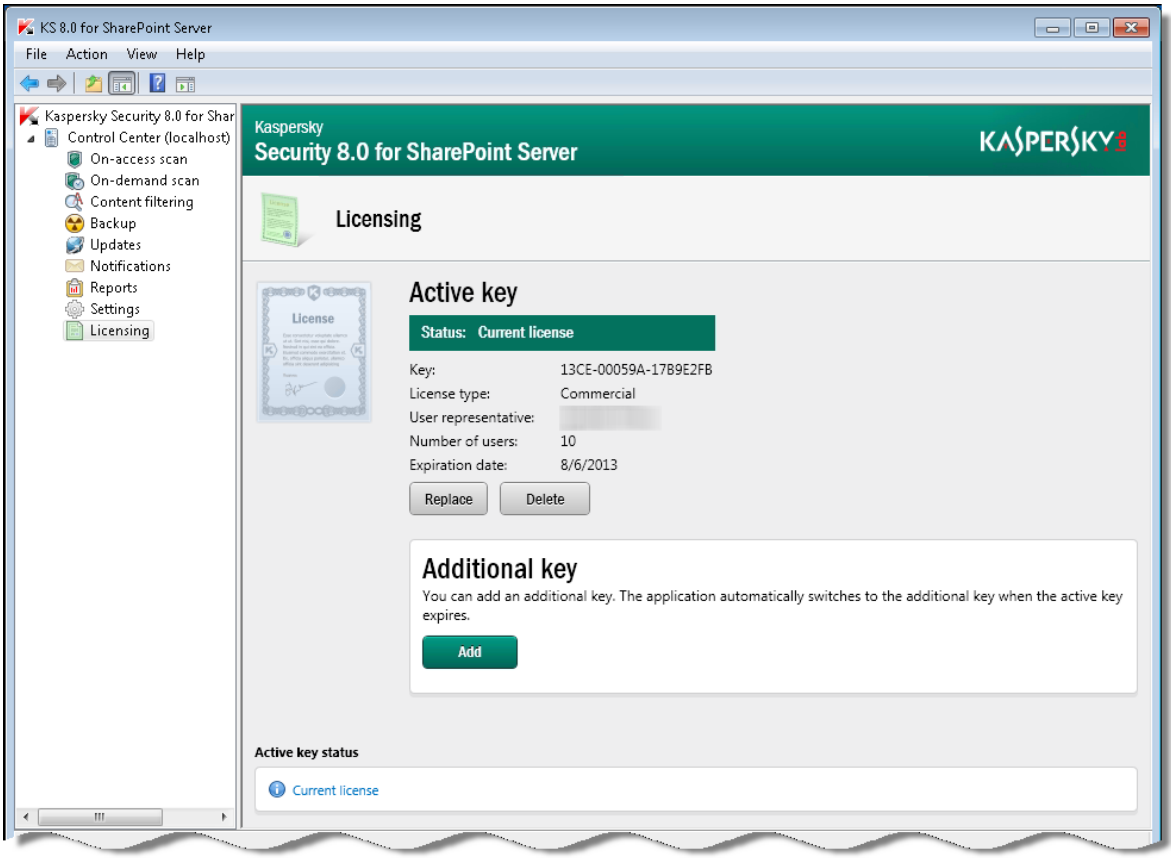
This section provides instructions for managing keys and describes settings of the expiring license notification.

IN THIS SECTION:

VIEWING INFORMATION ABOUT KEYS

➡ *To view information about the keys used by the application:*

1. Start Administration Console of the application.
2. In Administration Console tree select the necessary server node and then the **Licensing** node (see the figure below).



Active key

Status: Current license

Key: 13CE-00059A-17B9E2FB

License type: Commercial

User representative: [redacted]

Number of users: 10

Expiration date: 8/6/2013

Additional key

You can add an additional key. The application automatically switches to the additional key when the active key expires.

Active key status

Current license

*Figure 2:**Licensing** node*

You can use the details pane to view information about license keys that have been added. The following information about the active and additional keys is displayed:

- **Key**. A unique alphanumeric sequence needed to receive technical support from Kaspersky Lab.
- **License type**. Trial or commercial.
- **Representative**. Name of the representative of the company that executed the agreement to purchase the application.
- **Number of users**. The maximum number of employees with access to the SharePoint server protected by the application.
- **Expiration date**. License expiration date.

The table summarizes information about the key status on all SharePoint servers of the farm.

> If Kaspersky Security is installed on a standalone SharePoint server, key status information is displayed in the **Protection of farm servers** section in the details pane of the **Control Center (<Server name>)** node.

REPLACING A KEY

You can replace an active key with a key that has a longer validity period or allows more users of Kaspersky Security (if any).

Replacing an active key does not interfere with on-access scans, on-demand scan tasks, or database updates.

To replace the active key for Kaspersky Security:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. Click the **Replace** button in the details pane.
3. In the displayed **File name** dialog specify path to the key file (file with the .key extension) and click **Open**.

To replace an additional key:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. In the details pane, click the **Replace** button in the **Additional key** section.
3. In the displayed **File name** dialog specify path to the key file (file with the .key extension) and click **Open**.

REMOVING A KEY

To remove a key for Kaspersky Security:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. In the details pane, click the **Delete** button in the **Active key** or **Additional key** section.

> When Kaspersky Security is installed on a SharePoint farm and a key is removed from one SharePoint server within the farm, it is also removed from all servers of the SharePoint farm.

NOTIFICATION ABOUT LICENSE EXPIRY

The application verifies compliance with the license agreement after every database update.

The procedure can reveal the following problems with the license or keys:

- the key is not added;
- the license expires in several days;
- the license expired;
- the active key was found in the black list.

After checking the license, the application records the results of the check in the log and sends a notification to the administrator's email address and additional addresses (if notification settings are configured) about the licensing and key problems detected. By default, the application sends an expiring license notification 30 days before license expiry. You can set up a later notification date.

➧ *To configure the delivery of the Kaspersky Security license expiry notifications:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Notifications** node.
2. In the **Licensing** settings in the details pane, specify the email addresses where the notifications should be sent:
   - **Notify the Administrator about events related to the keys**. Notifications are sent to the administrator's email address specified in the **Settings node** (see section "**Configuring the application settings**" on page 94).
   - **Additional addresses**. Notifications will be sent to the email addresses specified in the field to the right.
3. In the details pane, specify in the field **Notify about license expiry in** the number of days in advance of license expiry that you want to be notified.
4. Click the **Save** button.

GETTING STARTED

This section describes the procedure for starting Administration Console and connecting servers to the SharePoint server.

IN THIS SECTION:

STARTING ADMINISTRATION CONSOLE

The services of Kaspersky Security start automatically during the operating system start-up. Administration Console is started manually.

➧ *To start Administration Console, perform the following steps:*

1. In the **Start** menu select **Programs.**
2. Select the **Kaspersky Security 8.0 for SharePoint Server** folder in the list of programs.
3. Select **Kaspersky Security 8.0 for SharePoint Server** in the menu.

When Administration Console starts, the snap-in of Kaspersky Security connects to MMC, so the console tree displays the application icon and the node of **Kaspersky Security 8.0 for SharePoint Server**.

After starting Administration Console, you can connect Administration Console to a SharePoint server (see section "Connecting Administration Console to a SharePoint server" on page 31).

To start Administration Console and manage the application, your account must have the administrator rights on the computer where Administration Console is started, and it must be a member of the Farm Administrators group.

CONNECTING ADMINISTRATION CONSOLE TO A SHAREPOINT SERVER

➧ *To connect Administration Console to a SharePoint server:*

1. Start Administration Console.
2. Select in Administration Console tree the node of **Kaspersky Security 8.0 for SharePoint Server**.
3. Click the **Connect to server** button in the details pane.
4. Select the appropriate option in the displayed dialog:
    - **Local computer**. Administration Console will be connected to the computer where it is installed (localhost).

- **Other computer**. Administration Console will connect to the specified SharePoint server to manage the application. If you select this option, use one of the following methods to specify the server name:
    - Click **Browse** and select the computer from the list in the displayed dialog.
    - Enter the server name manually as an IP address (in IPv4 or IPv6 notation) or DNS name.

5. Click **OK**.

   The specified server is added to Administration Console, and appears in the console tree.

To start Administration Console and manage the application, your account must have the administrator rights on the computer where Administration Console is started, and it must be a member of the Farm Administrators group.

CONNECTING ADMINISTRATION CONSOLE TO A SHAREPOINT FARM WHEN UPDATING KASPERSKY SECURITY

If Kaspersky Security is installed on SharePoint farm, you can connect Administration Console to any of the SharePoint farm servers.

When Kaspersky Security is being upgraded on SharePoint farm servers, it is not recommended to perform any operations with the application until the upgrade has been completed on all SharePoint farm servers.

If you need to use the application before completing the upgrade on all SharePoint farm servers, be sure to use the matching versions of Administration Console and the application on the SharePoint server. Administration Console of the previous version should be connected to server with the application version that has not been upgraded, and Administration Console of the new version should be connected to servers with upgraded Kaspersky Security.

During the application upgrade process, Anti-Virus databases are rolled back automatically. For the safety of your computer, you are advised to start the database update after completing the application upgrade.

When the application upgrade is started, the **I accept the KSN agreement and I want to use KSN** check box is automatically cleared in Kaspersky Security settings.

DATABASE UPDATE

This section describes how to configure database updates for Kaspersky Security, how to schedule automatic updates, and how to select and connect to update sources. It also includes information about how to configure each individual SharePoint server within a farm, and how to propagate global settings to all SharePoint servers in that farm.

IN THIS SECTION:

ABOUT DATABASE UPDATES

Kaspersky Security database updates keep SharePoint servers protected against new viruses and other threats. Databases contain the latest information about threats and ways to neutralize them.

Databases contain descriptions of all currently known malicious programs and methods to disinfect them, descriptions of software that intruders can use to harm a computer or user data, and also the Content filtering categories developed by Kaspersky Lab and used to check file content.

It is important to keep all databases up to date. You are advised to update the databases as soon as you install the application because the databases included in the distribution kit will already be out of date. The databases on Kaspersky Lab's update servers are updated every hour.

Databases can be updated from the following sources:

- Kaspersky Lab's update servers on the Internet
- Local updates source, such as a local or a network folder
- Another HTTP or FTP server, such as your Intranet server

The updating is performed either manually or automatically, according to a schedule. After the files are copied from the specified update source, the application automatically connects to the new databases.

For added protection of SharePoint files, you can use the Kaspersky Security Network service in addition to database updates (see section "About participation in Kaspersky Security Network" on page 94). This service provides up-to-date information about threats and malware before they have been included in Anti-Virus and Anti-Phishing databases.

During setup on several SharePoint farm servers, you can define local update settings (see section "Configuring the local database update settings on servers of the farm" on page 36) for each individual server or propagate the global update settings (see section "Propagating global database update settings to farm servers" on page 37) to all servers.

During the application upgrade process, Anti-Virus databases are rolled back automatically. For the safety of your computer, you are advised to start the database update after completing the application upgrade.

VIEWING THE INFORMATION ABOUT UPDATES TO THE ANTI-VIRUS DATABASE

To view the information about database updates:

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node.

2. In the details pane, go to the **Database update settings** tab.

   You will see a table with information about database updates on each SharePoint farm server. The table contains the following columns:

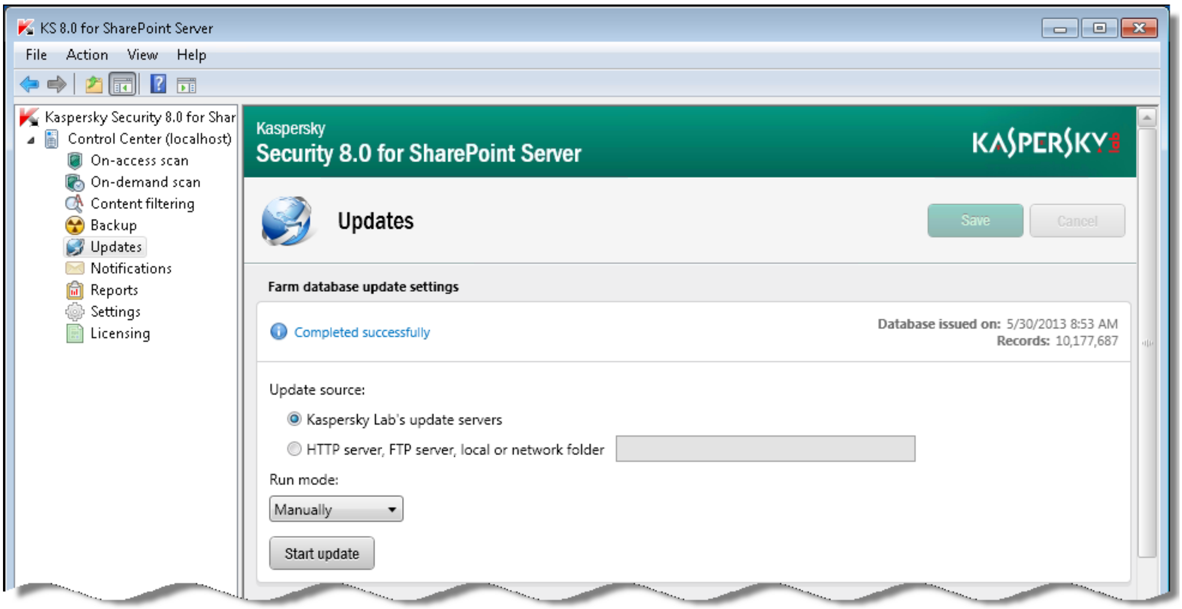
   - **Server name**. Server within a SharePoint farm, on which Kaspersky Security is installed.
   - **Status of the last database update**. The result of the last database update.
   - **Database release date (UTC)**. The time when databases currently used by the application were published on Kaspersky Lab servers.
   - **Time of last database update**. The time of the latest database update on the server.
   - **Settings**. Update settings used on the server (local or global).

If Kaspersky Security is installed on a standalone SharePoint server, update-related information is displayed in the details pane of the **Database update settings** section, not on the **Database update settings** tab.

CONFIGURING AUTOMATIC DATABASE UPDATES

To configure automatic database updates:

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node (see the figure below).



Farm database update settings

Completed successfully

Database issued on: 5/30/2013 8:53 AM
Records: 10,177,687

Update source:

● Kaspersky Lab's update servers

○ HTTP server, FTP server, local or network folder

Run mode:

Manually

Start update

*Figure 3:**Updates** node*

2. In the details pane, select the **General** tab and in the **Database update settings** section select the source of database updates:

   - **Kaspersky Lab's update servers**, to download updates from the servers of Kaspersky Lab.
   - **HTTP server, FTP server, local or network folder**, to download updates from any of these sources.

     If you select this option, specify in the corresponding text box the server address, local or network folder.

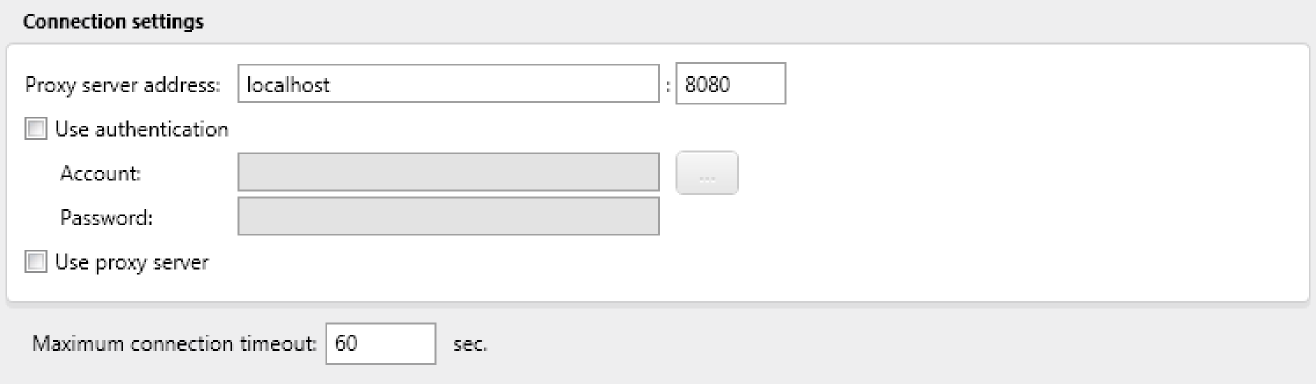
> If Kaspersky Security is installed on a standalone SharePoint server, the update source is selected in the **Database update settings** section of the details pane, which appears on selecting the **Updates** node in Administration Console tree.

3. The **Run mode** drop-down list lets you specify the database update schedule:

   - **Manually**. The update starts when you click the **Start database update on all farm servers** button.
   - **Periodically**. The update starts at the specified intervals.
   - **Daily**. The update starts at the specified time (the local time of the SharePoint server is used).
   - **On selected day**. The update starts on the specified days of the week.

> If Kaspersky Security is installed on a standalone SharePoint server, run mode for automatic database updates is configured in the **Database update settings** section of the details pane, not on the tab.

4. Specify the required connection settings in the **Connection settings** section (see figure below):



Connection settings

Proxy server address: localhost : 8080

□ Use authentication

Account: ...

Password:

□ Use proxy server

Maximum connection timeout: 60 sec.

*Figure 4:**Connection settings** section*

- If you connect to the Internet using a proxy server, check the **Use proxy server** box and specify the proxy server address and number of the port used for connection. Default proxy port number is 8080.
- If the proxy server requires authentication, specify the login name and password of the user account. To do this, check the **Use authentication** box and fill in the **Account** and **Password** fields.
- Specify the timeout duration in the **Maximum connection wait time** field. The default connection timeout is 60 seconds. By default, the timeout is set to 60 seconds.

  This proxy server is used for data exchange with the KSN cloud service when KSN protection is enabled (see section "Configuring KSN protection settings" on page 95).

> If Kaspersky Security is installed on a standalone SharePoint server, connection settings should be defined in the details pane, namely in the **Connection settings** section displayed after selection of the **Updates** node in the console tree.

5. Click the **Save** button.

CONFIGURING THE LOCAL DATABASE UPDATE SETTINGS ON SHAREPOINT SERVERS OF THE FARM

➧ *To configure the local database update settings on a SharePoint server within a farm:*

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node.

2. In the details pane, go to the **Update settings of servers** tab, select the necessary server in the table and click the button **Modify local settings**.

3. Use the displayed **Server settings** window to select in the **Database update settings** configuration section the source of updates:

   - **Kaspersky Lab's update servers**, to download updates from the servers of Kaspersky Lab.

   - **HTTP server, FTP server, local or network folder**, to download updates from any of these sources.

     If you select this option, enter the server address, local or network folder in the entry field.

4. In the **Database update settings** section, use the **Run mode** drop-down list to configure the database update schedule:

   - **Manually**. The update starts when you click the **Start update** button.

   - **Periodically**. The update starts at the specified intervals.

   - **Daily**. The update starts at the specified time (the local time of the SharePoint server is used).

   - **On selected day**. The update starts on the specified days of the week.

5. Use the **Connection settings** section to configure the connection:

   - If you connect to the Internet via a proxy server, select the **Use proxy server** check box and specify the proxy server address and number of the port used for connection. Default proxy port number is 8080.

   - If the proxy server requires authentication, specify the login name and password of the user account. To do this, check the **Use authentication** box and fill in the **Account** and **Password** fields.

   - Specify the timeout duration in the **Maximum connection wait time** field. The default connection timeout is 60 seconds. By default, the timeout is set to 60 seconds.

6. Click the **Save** button.

PROPAGATING GLOBAL DATABASE UPDATE SETTINGS TO SHAREPOINT FARM SERVERS

➡ *To apply the global database update settings on all SharePoint servers of the farm:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Updates** node.

2. In the details pane, go to the **Update settings of servers** tab, select the necessary server in the table and click the button **Propagate global settings**.

ON-ACCESS SCAN

This section contains information about automatic scanning of files as they are uploaded to the server or downloaded from the server to the user's computer. It describes the operating mechanism of on-access scanning and provides instructions for configuring Anti-Virus protection and Content filtering settings.

IN THIS SECTION:

ABOUT ON-ACCESS SCAN

On-access scan is a scan of files on a SharePoint server and SharePoint web objects as they are uploaded to the server or downloaded from the server to the user's computer.

Kaspersky Security performs on-access scan on:

- Files uploaded by the user to the SharePoint server;
- Files copied from the SharePoint server to the computer;
- SharePoint web objects (such as wiki pages and forums hosted on the SharePoint server) when they are created or modified.

During on-access scanning, Kaspersky Security performs:

1. Anti-Virus file scanning in accordance with the scan exclusions settings (see section "Creating on-access anti-virus scanning exclusions" on page 48).
2. Scanning of files for fragments of malicious code that exploits system vulnerabilities (see section "Enabling and disabling ZETA Shield technology" on page 95).
3. Scanning for unwanted file formats and unwanted file names (see section "Configuring additional settings for on-access Content filtering" on page 46).

4. Scanning of files and SharePoint web objects for unwanted content (see section "Configuring additional settings for on-access Content filtering" on page 46).

5. Checking of URLs contained in web content against a database of malicious and phishing URLs (see section "Enabling and disabling web content scanning for phishing" on page 43).

Based on the scan results, the application processes the file by taking the actions configured in the general on-access scan settings (see section "Configuring object processing rules for on-access scanning" on page 44).

If a file has been blocked by Content filtering, the application does not perform Anti-Virus scanning of this file. Alternatively, if a file has been blocked during an Anti-Virus scan, the application does not apply Content filtering to the file.

You can enable or disable application operations during on-access scanning.

Status labels assigned to files following on-access scan

Based on the results of on-access scanning, the application assigns one of the following status labels to the file:

- *Not infected*. No threats detected in the file.
- *Infected*. A file a segment of whose code fully matches a code segment of a known threat.
- *Potentially infected*. A file whose code contains a modified segment of code of a known threat, or a file resembling a threat in the way it behaves.
- *Password-protected*. A password-protected archive.
- *Corrupted.* The file cannot be read by Kaspersky Security.

Based on the results of Content filtering, the application assigns one of the following status labels to the file:

- *Allowed*. There is no unwanted content in the file.
- *Forbidden format*. The file has an unwanted format.
- *Forbidden mask*. The file name contains an unwanted mask.
- *Forbidden content*. The file has been found to contain unwanted words and phrases.

Based on the results of Content filtering, the application assigns one of the following status labels to the SharePoint web object:

- *Allowed.* The SharePoint web object does not contain unwanted content, malicious or phishing URLs.
- *Forbidden content*. The SharePoint web object has been found to contain malicious / phishing URLs or unwanted content.

ABOUT PHISHING SCAN

Phishing scan is a feature of Kaspersky Security designed to protect personal data of users.

While scanning the content of SharePoint web objects, the application checks links against lists of malicious and phishing URLs.

By checking links against a list of malicious URLs, the application is able to detect URLs leading to infected sites. Malicious URLs can appear in the message body as advertising that encourages you to find out more about a product by clicking the link. The URL takes you to a website with viruses, and the computer gets infected with viruses. The computer is infiltrated by viruses and malware that can access your private data and relay it to criminals.

By checking links against a list of phishing URLs, the application is able to detect links leading to fraudulent sites. A phishing attack can be disguised, for example, as a letter from your bank with a link to its official website. The link takes you to an exact copy of the bank's website where you can even see the bank site's address in the browser despite actually being on a spoofed website. From this point forward, all of your actions on the site are tracked and can be used to steal your private data.

A phishing scan of SharePoint web objects detects malicious and phishing URLs embedded in the text of web objects. Malicious and phishing URLs are designed to steal your personal data or information entered in a web form. The application performs a phishing scan when a SharePoint web object is created or modified. If the phishing scan detects at least one URL appearing on lists of malicious and phishing URLs, the application assigns the *Phishing* status label to the web object.

On detecting a malicious or phishing URL in a SharePoint web object, the application performs the action configured for Content filtering (see section "Configuring general on-access scan settings" on page 43). If the action is set to **Block**, the application shows a dialog saying that web content cannot be created or modified.

To protect a SharePoint server or servers against phishing, the application uses a list of URLs that have been labeled as malicious or phishing URLs by Kaspersky Lab. The database is regularly updated and is part of the Kaspersky Security delivery kit.

You can use the *Kaspersky Security Network service* for additional protection of a SharePoint server or servers against phishing (see section "*About participation in Kaspersky Security Network*" on page 94). It uses cloud computing technology that provides up-to-the-minute information about threats before they have been included in Kaspersky Lab anti-phishing databases.

KASPERSKY SECURITY OPERATION DEPENDING UPON THE SHAREPOINT SERVER SETTINGS

Kaspersky Security in on-access scan mode depends on the Anti-Virus scan settings configured on the SharePoint server.

Scanning files uploaded to a SharePoint server

➡ *To enable anti-virus scanning of files as they are uploaded to a server,*

select the **Scan documents on upload** check box in the anti-virus scan settings on the SharePoint server.

You can view and configure the anti-virus scan settings on the SharePoint server in the details pane of the **Control Center (<Server name>)** node on the **Events and statistics tab (see section "SharePoint settings" on page 22)** and in the details pane of the **On-access scan** node on the **General** tab (see section "**Configuring general on-access scan settings**" on page 43).

Depending on the anti-virus scan settings configured on the SharePoint server, the application takes one of the following actions on a file uploaded to the SharePoint server:

- **Block**. Kaspersky Security blocks the file in the following cases:
  - The **Attempt to disinfect infected documents** check box is cleared in the Anti-Virus scan settings of the SharePoint server
  - The **Block** action is selected in the on-access scan settings of Kaspersky Security
  - The **Disinfect** action is selected in the on-access scan settings of Kaspersky Security, but the file cannot be disinfected
- **Disinfect**. Kaspersky Security attempts to disinfect the file in the following cases:
  - The **Attempt to disinfect infected documents** check box is selected in the Anti-Virus scan settings of the SharePoint server

    - The **Disinfect** action is selected in the on-access scan settings of Kaspersky Security

- **Skip**. Kaspersky Security skips the file with viruses or unwanted content if the **Skip** action is selected in on-access scan settings.

Scanning files downloaded from a SharePoint server to the computer

➧ *To enable anti-virus scanning of files as they are downloaded from a server to the user's computer,*

select the **Scan documents on download** check box in the anti-virus scan settings on the SharePoint server.

Depending on the anti-virus scan settings configured on the SharePoint server, the application takes one of the following actions on a file downloaded from the SharePoint server:

- **Block**. Kaspersky Security blocks the file if the user who is not a member of the server administrators group tries to download the file from the server, and one of the following conditions is met:
    - The **Attempt to disinfect infected documents** check box is cleared in the Anti-Virus scan settings of the SharePoint server
    - The **Block** action is selected in the on-access scan settings of Kaspersky Security
    - the **Disinfect** action is selected in the on-access scan settings of Kaspersky Security, but the file cannot be disinfected, and the **Allow users to download infected documents** check box is cleared in the SharePoint server settings.
- **Disinfect**. Kaspersky Security attempts to disinfect the file in the following cases:
    - The **Attempt to disinfect infected documents** check box is selected in the Anti-Virus scan settings of the SharePoint server
    - The **Disinfect** action is selected in the on-access scan settings of Kaspersky Security
- **Warn about infected file downloads**. Kaspersky Security displays a warning about a file with viral or unwanted content if the user trying to access the dangerous file is a member of the SharePoint server administrators group or the **Allow users to download infected documents** check box is selected in the SharePoint settings, and one of the following conditions is met:
    - The **Attempt to disinfect infected documents** check box is cleared in the Anti-Virus scan settings of the SharePoint server
    - The **Block** action is selected in the on-access scan settings of Kaspersky Security
    - The **Disinfect** action is selected in the on-access scan settings of Kaspersky Security, but the file cannot be disinfected

ENABLING AND DISABLING ON-ACCESS ANTI-VIRUS SCANNING

➧ *To enable / disable on-access Anti-Virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.
2. Do one of the following on the **General** tab:
    - Select the **Enable Anti-Virus scan** check box if you want the application to perform on-access anti-virus scanning of the file.

- Clear the **Run Anti-Virus scan** check box if you do not want the application to perform on-access anti-virus scanning of the file.

3. Click the **Save** button.

ENABLING AND DISABLING ON-ACCESS CONTENT FILTERING

➡ *To enable / disable on-access Content filtering:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. Do one of the following on the **General** tab:

   - Select the **Enable Content filtering** check box if you want the application to perform content filtering of the file during on-access scanning.

   - Clear the **Enable Content filtering** check box if you do not want the application to perform content filtering of the file during on-access scanning.

3. Click the **Save** button.

> To ensure a proper functioning of Content Filtering, the Kaspersky Security account should have the websites collection administrator rights (for all websites collection) and the administrator rights in the SQL database that contains the websites collection.

ENABLING AND DISABLING SHAREPOINT WEB OBJECT SCANNING

➡ *To enable or disable the scanning SharePoint web objects:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. Do one of the following on the **General** tab:

   - Select the **Scan SharePoint web content** check box if you want the application to scan SharePoint web objects when they are created or modified.

   - Clear the **Scan SharePoint web content** check box if you do not want the application to scan SharePoint web objects when they are created or modified.

   > Kaspersky Security scans SharePoint web objects if Content filtering is enabled (the **Enable Content filtering** check box is selected).

   If the **Scan SharePoint web content** check box is selected, the application scans SharePoint web objects that are created or modified for unwanted words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the content filtering settings (see section "Configuring additional settings for on-access content filtering" on page 46).

On detecting unwanted content in a SharePoint web object, the application makes a corresponding record in the application log and the Windows event log. Kaspersky Security does not save the SharePoint web objects or move them to Backup. The application shows a message that such SharePoint web object cannot be saved or modified.

> If Kaspersky Security blocks a SharePoint web object under Microsoft SharePoint Server 2010, the application may fail to save the changes made to this SharePoint web object or the newly created SharePoint web object.

3. Click the **Save** button.

ENABLING AND DISABLING ANTI-PHISHING SCANNING OF WEB CONTENT

➧ *To enable or disable Anti-Phishing scanning of web content:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. Do one of the following on the **General** tab in the **Content filtering** section:

   - Select the **Scan content of SharePoint web objects for phishing** check box to have the application scan SharePoint content as it is created or modified for URLs appearing on lists of malicious or phishing URLs.

   - Clear the **Scan content of SharePoint web objects for phishing** check box to stop the application from scanning SharePoint content as it is created or modified for URLs appearing on lists of malicious or phishing URLs.

   Kaspersky Security scans web content for malicious and phishing URLs if Content filtering is enabled (the **Enable Content filtering** check box is selected) and scanning of SharePoint web objects is enabled (the **Scan SharePoint web objects** check box is selected).

   If the **Scan content of SharePoint web objects for phishing** check box is selected, the application checks URLs against the Kaspersky Lab database of malicious and phishing URLs when web content is created or modified. If Kaspersky Security Network is used to protect a server or servers, information about the malicious or phishing URL can be relayed to the KSN service (see section "Configuring KSN protection settings" on page 95)).

   On detecting a phishing threat in a SharePoint web object, the application logs information about it in **Reports** (see page 87).

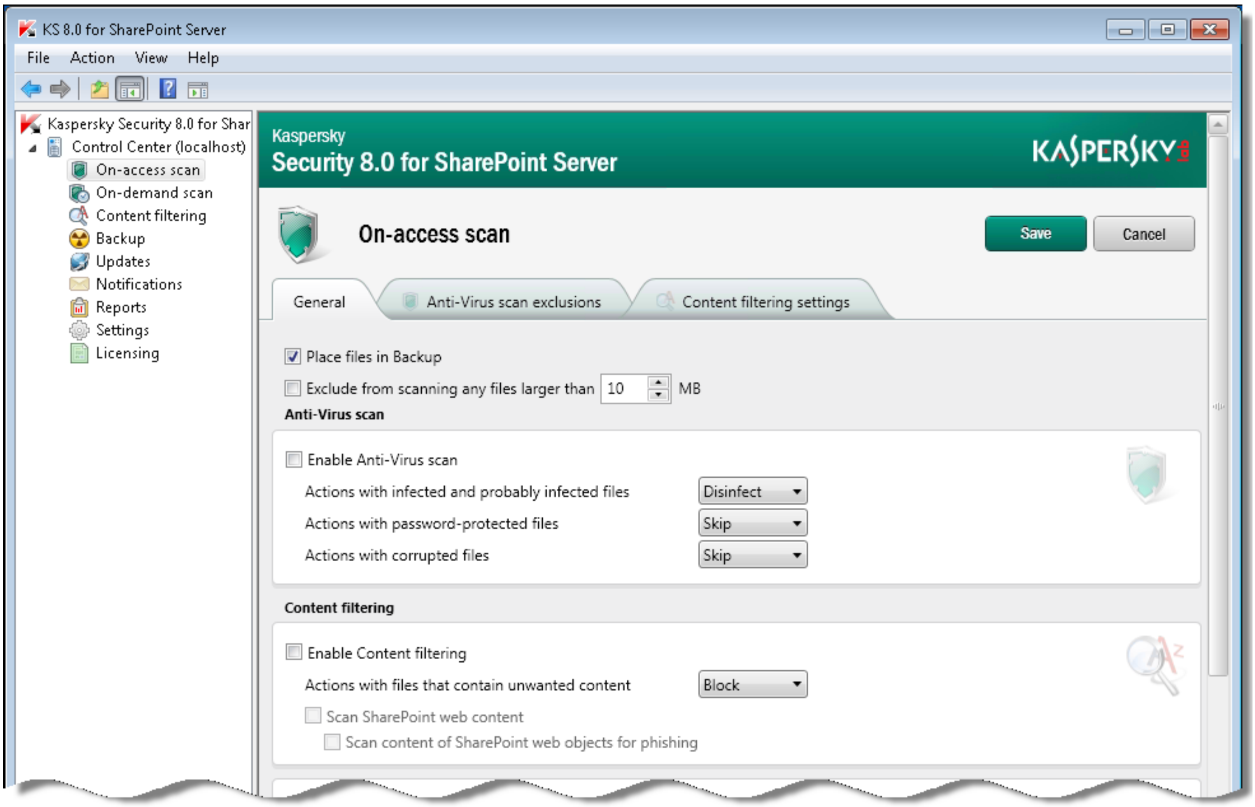
3. Click the **Save** button.

CONFIGURING GENERAL ON-ACCESS SCAN SETTINGS

➧ *To define general on-access scan settings:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. Select the **General** tab in the results pane (see figure below):



KS 8.0 for SharePoint Server
File
Action
View
Help
Kaspersky Security 8.0 for Shar
Control Center (localhost)
On-access scan
On-demand scan
Content filtering
Backup
Updates
Notifications
Reports
Settings
Licensing
Kaspersky
Security 8.0 for SharePoint Server
KASPERSKY
On-access scan
Save
Cancel
General
Anti-Virus scan exclusions
Content filtering settings

☑ Place files in Backup

□ Exclude from scanning any files larger than 10 MB

Anti-Virus scan

□ Enable Anti-Virus scan

Actions with infected and probably infected files	Disinfect
Actions with password-protected files	Skip
Actions with corrupted files	Skip

Content filtering

□ Enable Content filtering

Actions with files that contain unwanted content	Block

□ Scan SharePoint web content

□ Scan content of SharePoint web objects for phishing

Figure 5: General On-access scan settings

3. Select the **Move files to Backup** check box if you want Kaspersky Security to create Backup copies of files that have been blocked after Anti-Virus scanning and Content filtering.

4. If you want to restrict the size of files to be scanned, select the **Exclude from scanning any files larger than** check box, and specify the maximum size of files to scan (in megabytes). The default value is 10 MB.

5. Click the **Save** button.

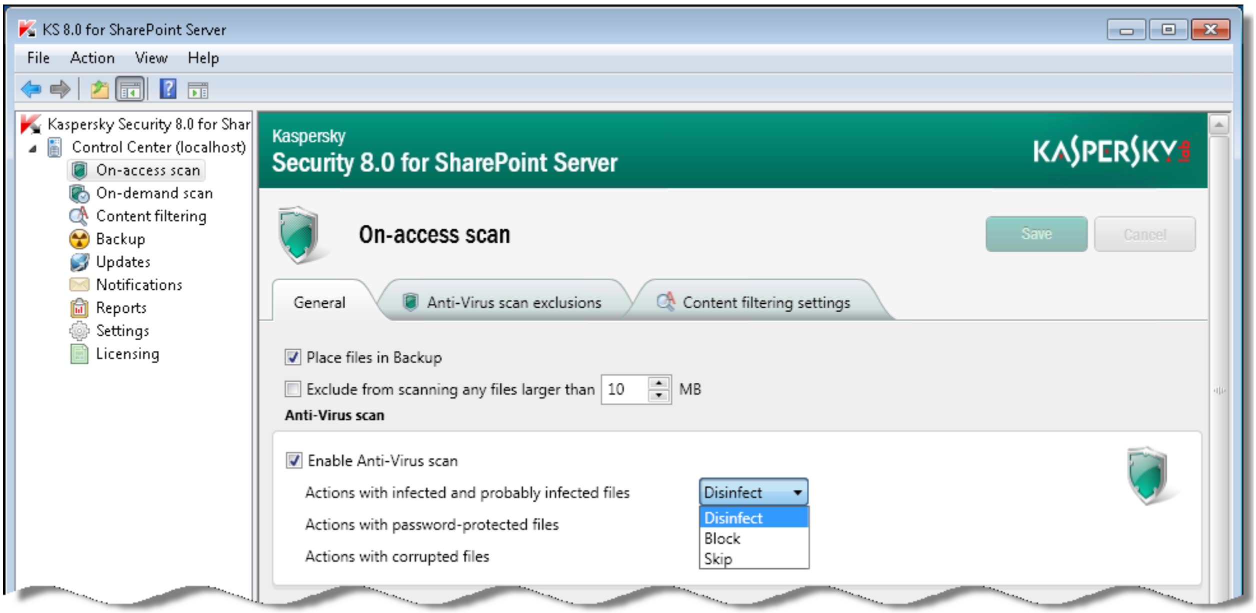
CONFIGURING OBJECT PROCESSING RULES FOR ON-ACCESS SCANNING

Kaspersky Security will handle infected, probably infected, corrupted and password-protected files depending on the values of Anti-Virus scan settings of the SharePoint server (see section "Kaspersky Security operation depending upon the SharePoint server settings" on page 40).

➧ *To create object processing rules for anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node, and in the details pane click the **General** tab.

2. In the **Anti-Virus scan** section, open the **What to do with infected and potentially infected files** drop-down list and select one of the following actions (see the figure below):



KS 8.0 for SharePoint Server
File Action View Help
Kaspersky Security 8.0 for Shar
Control Center (localhost)
On-access scan
On-demand scan
Content filtering
Backup
Updates
Notifications
Reports
Settings
Licensing
Kaspersky
Security 8.0 for SharePoint Server
KASPERSKY
On-access scan
Save
Cancel
General
Anti-Virus scan exclusions
Content filtering settings

☑ Place files in Backup

□ Exclude from scanning any files larger than 10 MB

Anti-Virus scan

☑ Enable Anti-Virus scan

Actions with infected and probably infected files: Disinfect

Actions with password-protected files

Actions with corrupted files

Figure 6: Object processing rules to be used during anti-virus scanning

- **Disinfect**. Kaspersky Security attempts to disinfect the file. If the file cannot be disinfected, Kaspersky Security blocks it (the file is not uploaded to the SharePoint server or downloaded from the server to the user's computer).
- **Block**. Kaspersky Security blocks the file.
- **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.

3. In the **Anti-Virus scan** section, open the **What to do with password-protected files** drop-down list and select one of the following actions:

- **Block**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
- **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.

4. In the **Anti-Virus scan** section, open the **What to do with damaged files** drop-down list and select one of the following actions:

- **Block**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
- **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.

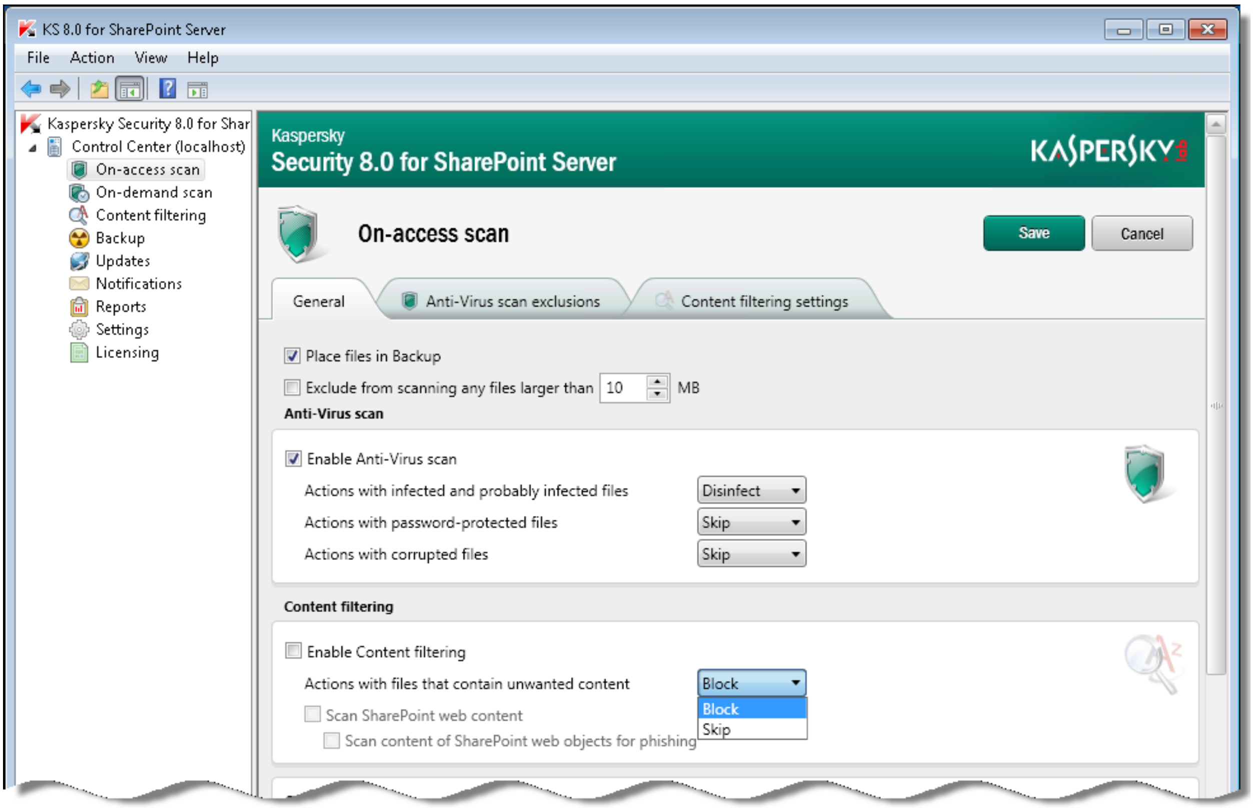
If the **Skip** option is selected, Kaspersky Security does not take any action on the file, but the file is assigned one of the status labels based on the scan results (see section "About on-access scan" on page 38). File information is recorded in reports (see page 87) and statistics (see section "Statistics" on page 24).

5. To save the changes, click **Save**.

To create object processing rules for Content filtering:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node, and in the details pane click the **General** tab.

2. In the **Content filtering** section, open the **What to do with files that contain unwanted content** drop-down list and select one of the following actions (see the figure below):



KS 8.0 for SharePoint Server
File
Action
View
Help
Kaspersky Security 8.0 for Shar
Control Center (localhost)
On-access scan
On-demand scan
Content filtering
Backup
Updates
Notifications
Reports
Settings
Licensing
Kaspersky
Security 8.0 for SharePoint Server
KASPERSKY
On-access scan
Save
Cancel
General
Anti-Virus scan exclusions
Content filtering settings

☑ Place files in Backup

☐ Exclude from scanning any files larger than 10 MB

Anti-Virus scan

☑ Enable Anti-Virus scan

Actions with infected and probably infected files: Disinfect

Actions with password-protected files: Skip

Actions with corrupted files: Skip

Content filtering

☐ Enable Content filtering

Actions with files that contain unwanted content: Block (Block, Skip)

☐ Scan SharePoint web content

☐ Scan content of SharePoint web objects for phishing

Figure 7: Object processing rules during content filtering

- **Block**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
- **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.

3. To save the changes, click **Save**.

If the **Skip** option is selected, Kaspersky Security does not take any action on the file, but the file is assigned one of the status labels based on the scan results (see section "About on-access scan" on page 38). Information about the file will be added to the reports and statistics.

CONFIGURING ADDITIONAL SETTINGS FOR ON-ACCESS CONTENT FILTERING

You can configure additional settings for on-access Content filtering: specify prohibited file formats, masks of unwanted file names, unwanted words or phrases.

To specify prohibited file formats:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. In the details pane, select the **Content filtering settings** tab (see figure below).

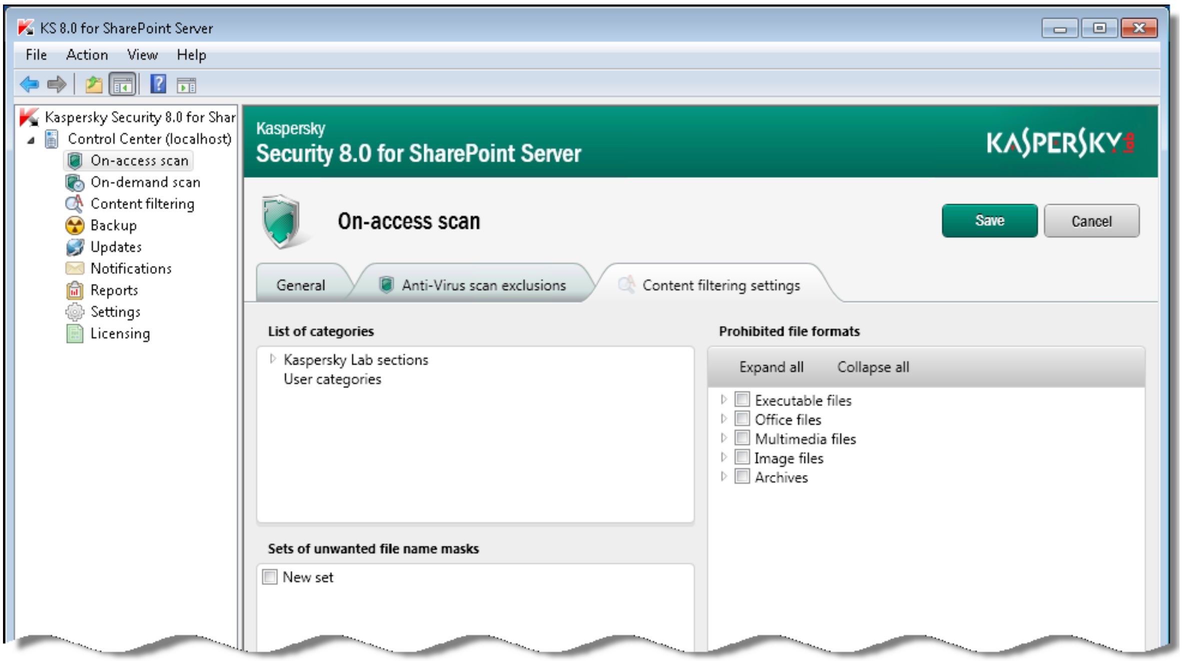


Figure 8: Content filtering settings during on-access scan

3. In the **Unwanted file formats** section, select the check boxes next to the unwanted file formats.

   You can manipulate the tree using the **Expand all** and **Collapse all** buttons.

4. To save the changes, click **Save**.

To specify the masks for unwanted file names:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. In the details pane, select the **Content filtering settings** tab.

3. In the **Sets of unwanted file name masks** field, select the check boxes next to the unwanted file masks.

> In the **Content filtering** node you can add and edit the sets of unwanted file name masks using the **Masks of unwanted file names** tab (see section "**Creating, renaming, and deleting a set of masks for unwanted file names**" on page 68).

4. To save the changes, click **Save**.

To define unwanted words and phrases:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. In the details pane, select the **Content filtering settings** tab.

3. In the **List of categories**, select check boxes opposite the categories of unwanted words and phrases.

> You can add and edit custom categories of unwanted words and expressions in the **Content filtering** node using the tab **Words and phrases** (see section "**Adding, changing, and deleting unwanted words and phrases in user categories**" on page 64).

4. To save the changes, click **Save**.

CREATING ON-ACCESS ANTI-VIRUS SCAN EXCLUSIONS

To reduce the load on the SharePoint server caused by on-access Anti-Virus scanning, you can specify file formats or file name masks to be excluded from scanning and set the maximum size of files to scan.

➧ *To exclude unwanted file formats from on-access anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.
2. Select the **Anti-Virus scan exclusions** tab in the details pane (see figure below).

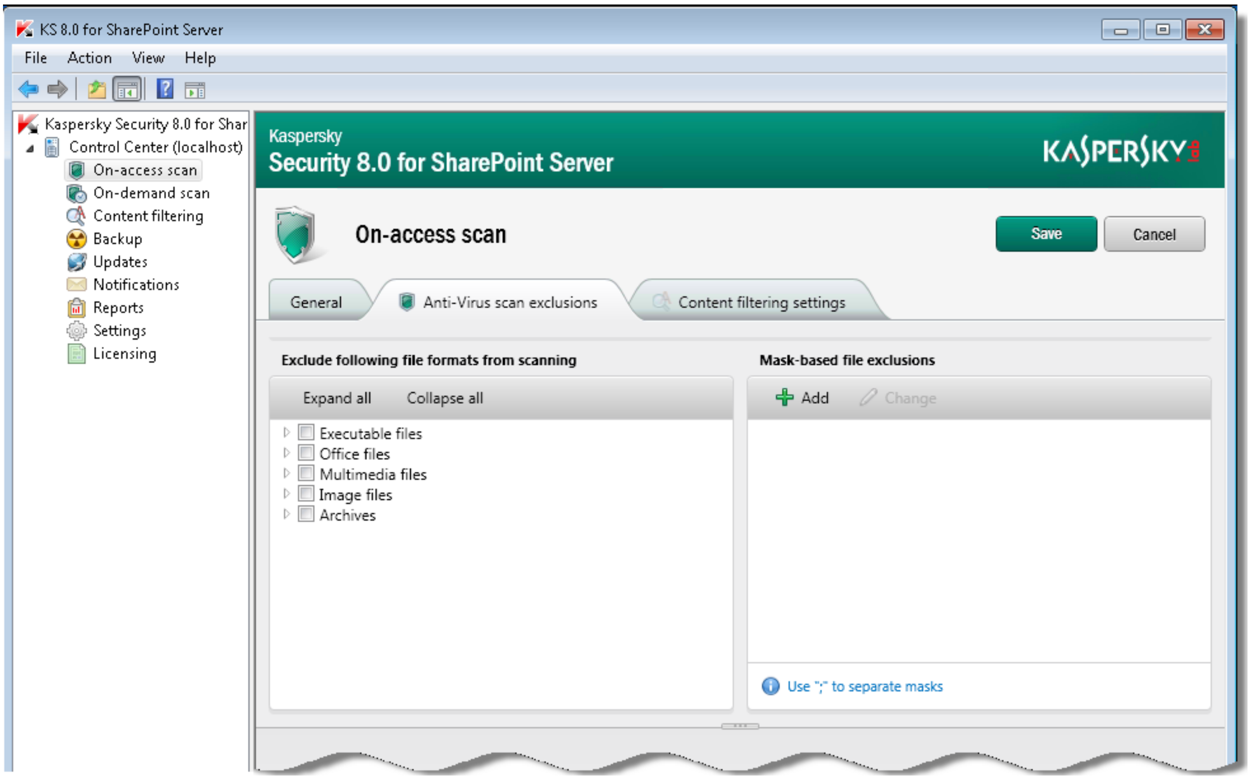

KS 8.0 for SharePoint Server
File
Action
View
Help
Kaspersky Security 8.0 for Shar
Control Center (localhost)
On-access scan
On-demand scan
Content filtering
Backup
Updates
Notifications
Reports
Settings
Licensing
Kaspersky
Security 8.0 for SharePoint Server
KASPERSKY
On-access scan
Save
Cancel
General
Anti-Virus scan exclusions
Content filtering settings
Exclude following file formats from scanning
Expand all
Collapse all
Executable files
Office files
Multimedia files
Image files
Archives
Mask-based file exclusions
Add
Change
Use ";" to separate masks

Figure 9: Creating on-access Anti-Virus scan exclusions

3. In the **Exclude following file formats from scanning** list, select check boxes next to the items in the file format tree corresponding to the formats you want to exclude.

   You can manipulate the tree using the **Expand all** and **Collapse all** buttons.

4. To save the changes, click **Save**.

➡ *To exclude files that match specific masks from Anti-Virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-access scan**.

2. Select the **Anti-Virus scan exclusions** tab in the details pane.

3. In the **Mask-based file exclusions** list, select check boxes next to file name masks to be excluded from the scan scope.

4. To add a mask to the list, click **Add** to open the **Adding file mask** dialog and enter the mask in the entry field. To save the changes and close the window, click **OK**. The mask appears in the **Mask-based file exclusions** field (see section "**File name mask creation rules**" on page 67).

   If you want to define several masks, use a semicolon as a delimiter.

5. To save the changes, click **Save**.

ON-DEMAND SCAN

This section provides detailed information about on-demand scan tasks and guidelines for creating, configuring and scheduling on-demand scan tasks.

IN THIS SECTION:

ABOUT ON-DEMAND SCANNING

On-demand scan is scanning of files on a SharePoint server, which is performed manually or according to a schedule created in advance.

Kaspersky Security performs on-demand scan on:

- files located on the SharePoint server and in areas of the SharePoint structure specified in the scan settings;
- all SharePoint web objects (such as wiki pages and forums hosted on the SharePoint server);
- SharePoint service files.

The application scans only the last versions of files and SharePoint web objects hosted on the SharePoint server.

During on-demand scanning, Kaspersky Security performs:

1. Anti-virus file scanning in accordance with the scan exclusions settings (see section "Creating on-demand anti-virus scan exclusions" on page 56).
2. Scanning of files for fragments of malicious code that are typical of exploits (see section "Enabling and disabling ZETA Shield technology" on page 95).
3. Scanning for unwanted file formats and unwanted file names (see section "Configuring additional settings for on-access Content filtering" on page 46).
4. Scanning of files and SharePoint web objects for unwanted content (see section "Configuring additional settings for on-access Content filtering" on page 46).

If a file has been blocked by Content filtering, the application does not perform Anti-Virus scanning of this file. Alternatively, if a file has been blocked following an Anti-Virus scan, the application does not apply Content filtering to the file.

Status labels assigned to files based on scan results

Based on the results of Anti-Virus scanning, Kaspersky Security assigns one of the following status labels to the file:

- *Not infected*. No threats detected in the file.
- *Infected*. A file a segment of whose code fully matches a code segment of a known threat.
- *Potentially infected*. A file whose code contains a modified segment of code of a known threat, or a file resembling a threat in the way it behaves.
- *Password-protected*. A password-protected archive.
- *Corrupted.* The file cannot be read by Kaspersky Security.

Based on the results of content filtering, Kaspersky Anti-Virus assigns one of the following status labels to the file:

- *Allowed.* There is no unwanted content in the file.
- *Forbidden format*. The file has an unwanted format.
- *Forbidden mask*. The file name contains an unwanted mask.
- *Forbidden content*. The file has been found to contain unwanted words and phrases.

Based on the results of content filtering, the application assigns one of the following status labels to the SharePoint web object:

- *Allowed.* The SharePoint web object does not contain unwanted content.
- *Forbidden content*. The SharePoint web object has been found to contain unwanted content.

On-demand scan tasks

To run an on-demand scan in Kaspersky Security, create an on-demand scan task or tasks (see section "Creating an on-demand scan task" on page 52). You can configure Anti-Virus scanning and Content filtering settings for each on-demand scan task, and define a schedule.

On-demand scan tasks can be run manually or scheduled to run automatically. After performing each scan task, the application generates a report (see section "Viewing an on-demand scan task report" on page 59).

The list of on-demand scan tasks is displayed in the results pane of the **On-demand scan task** node. The on-demand scan tasks that were not run or could not be run at the scheduled time are highlighted in red. Color highlighting is not used for other tasks.

The reasons for not running the tasks are displayed in the **Status** column:

- **Non-existent server.** Kaspersky Security Server has been deleted from the SharePoint server specified in the on-demand scan task settings. You can specify a different SharePoint server in the task settings.
- **Task not executed**. The SharePoint server specified in the on-demand scan task settings was not available at the time scheduled for the start of the task. The availability of the SharePoint server needs to be checked. You can run a task manually, if necessary.

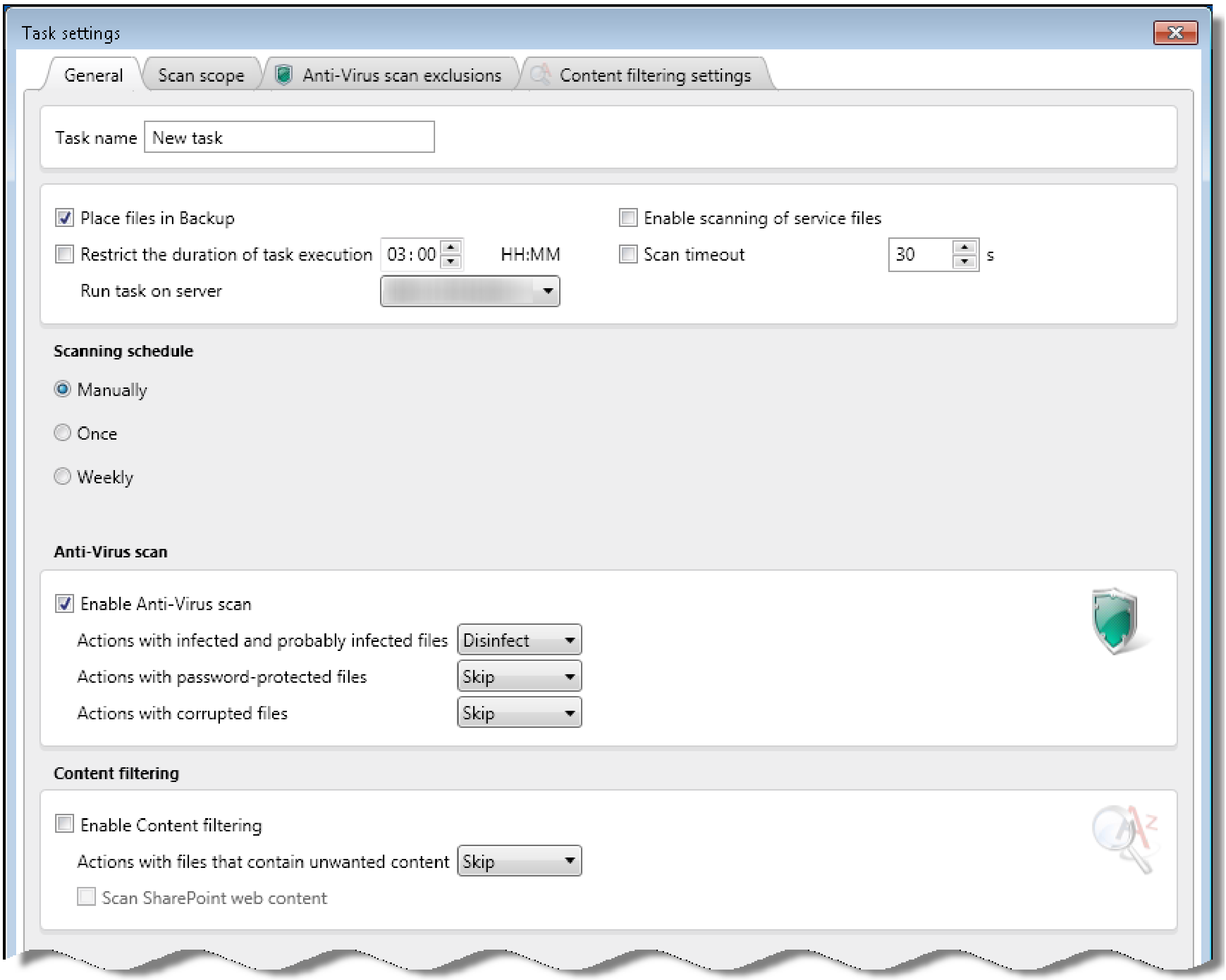
CREATING AN ON-DEMAND SCAN TASK

➧ *To create an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Click the **Create** button in the results pane.

   The **Task settings** window opens (see figure below).



Task name: New task

☑ Place files in Backup

□ Enable scanning of service files

□ Restrict the duration of task execution 03 : 00 HH:MM

□ Scan timeout 30 s

Run task on server [redacted]

Scanning schedule

● Manually

○ Once

○ Weekly

Anti-Virus scan

☑ Enable Anti-Virus scan

Actions with infected and probably infected files: Disinfect

Actions with password-protected files: Skip

Actions with corrupted files: Skip

Content filtering

□ Enable Content filtering

Actions with files that contain unwanted content: Skip

□ Scan SharePoint web content

Figure 10: Configuring general settings of on-demand scan tasks

3. Enter the **Task name** in the corresponding field.

4. Configure restrictions for the newly created on-demand scan task:

   - If you want Kaspersky Security to back up original files before processing, select the **Place files in Backup** check box.

   - If you want to restrict the duration of an on-demand scan task, check the box **Restrict the duration of task execution** and specify the maximum value in the box to the right.

   - If you want the application to scan SharePoint service files while performing the task, select the **Enable scanning of service files** check box.

- If you want to restrict scanning duration for individual files, select the **Scan timeout** check box and enter the time value (seconds) in the corresponding field to the right.

- If you want to run the task on a different SharePoint server, select the relevant SharePoint server in the **Run task on server** drop-down list.

5. Configure the schedule for the on-demand scan task in the **Scanning schedule** section:

   - If you want to run the on-demand scan task manually at your convenience, select **Manually**.

   - If you want the on-demand scan task to run once at the specified time, select **Once** and specify the date and time for task launch.

   - If you want the on-demand scan task to run automatically every week, select **Weekly** and specify the days and time for task launch.

   > If the **Once** or **Weekly** option is selected, the application uses the time set on the SharePoint server where the task will be run.

6. If necessary, in the **Anti-Virus scan** section, select the **Enable Anti-Virus scan** check box and configure actions to performed by the application on infected, potentially infected, password-protected, and corrupted files during the task:

   - in the **What to do with infected and potentially infected files** list, select the action:

     - **Disinfect**. Kaspersky Security attempts to disinfect an infected or potentially infected file. If the file cannot be disinfected, the application replaces it with a text file describing the reason for deletion.

     - **Delete**. Kaspersky Security replaces the infected or potentially infected file with a text file describing the reason for deletion.

     - **Skip**. Kaspersky Security does not perform any operations on the infected or potentially infected file.

   - in the **What to do with password-protected files** list, select the action:

     - **Delete**. Kaspersky Security replaces the password-protected file with a text file describing the reason for deletion.

     - **Skip**. Kaspersky Security does not perform any action on the password-protected file.

   - in the **What to do with damaged files** list, select the action:

     - **Delete**. Kaspersky Security replaces a corrupted file with a text file describing the reason for deletion of the original file.

     - **Skip**. Kaspersky Security does not perform any action on the corrupted file.

   > If the **Skip** option is selected, the application does not take any action on the file, but assigns one of the status labels to the file based on the scan results (see section "About on-demand scanning" on page 50). The application records the file details in reports and statistics.

7. If necessary, select the **Enable Content filtering** check box and select the action to be performed on files containing unwanted content in the **What to do with files that contain unwanted content** list:

   - **Delete**. Kaspersky Security replaces a file with unwanted content with a text file describing the reason for deletion of the original file.

> If Kaspersky Security detects unwanted content in a SharePoint service file, it does not delete this file. The application records information about unwanted content in the SharePoint service file in the task report and the application log.

- **Skip**. Kaspersky Security does not perform any action on the file containing unwanted content.

  > If the **Skip** option is selected, the application does not take any action on the file, but assigns one of the status labels to the file based on the scan results (see section "About on-demand scanning" on page 50). The application records the file details in reports and statistics.

8. If you want the application to scan SharePoint web objects (such as wiki pages and forums hosted on the SharePoint server) during Content filtering, select the **Scan SharePoint web content** check box.

   If the **Scan SharePoint web objects** check box is selected, the application scans SharePoint web objects for unwanted words or phrases included in Kaspersky Lab sections and user categories that are configured in the Content filtering node (see section "Configuring Content filtering" on page 57).

   If the application detects unwanted content in a SharePoint web object, it records information about this in the on-demand scan report (see section "Viewing an on-demand scan task report" on page 59) and the application log. Kaspersky Security does not delete the SharePoint web object or move it to Backup.

> To ensure a proper functioning of Content Filtering, the Kaspersky Security account should have the websites collection administrator rights (for all websites collection) and the administrator rights in the SQL database that contains the websites collection.

9. Click **OK**.

   The created task appears in the list of tasks in the results pane of the **On-demand scan** node.

You can configure additional settings for an on-demand scan task:

- Select or exclude areas of the SharePoint structure from the scan scope (see section "Selecting and excluding from on-demand scanning areas of the SharePoint structure" on page 54).
- Exclude certain file types, file formats, or file name masks from the anti-virus scan, restrict file scan duration (see section "Creating on-demand Anti-Virus scan exclusions" on page 56).
- Configure Content filtering (see section "Configuring Content filtering" on page 57).

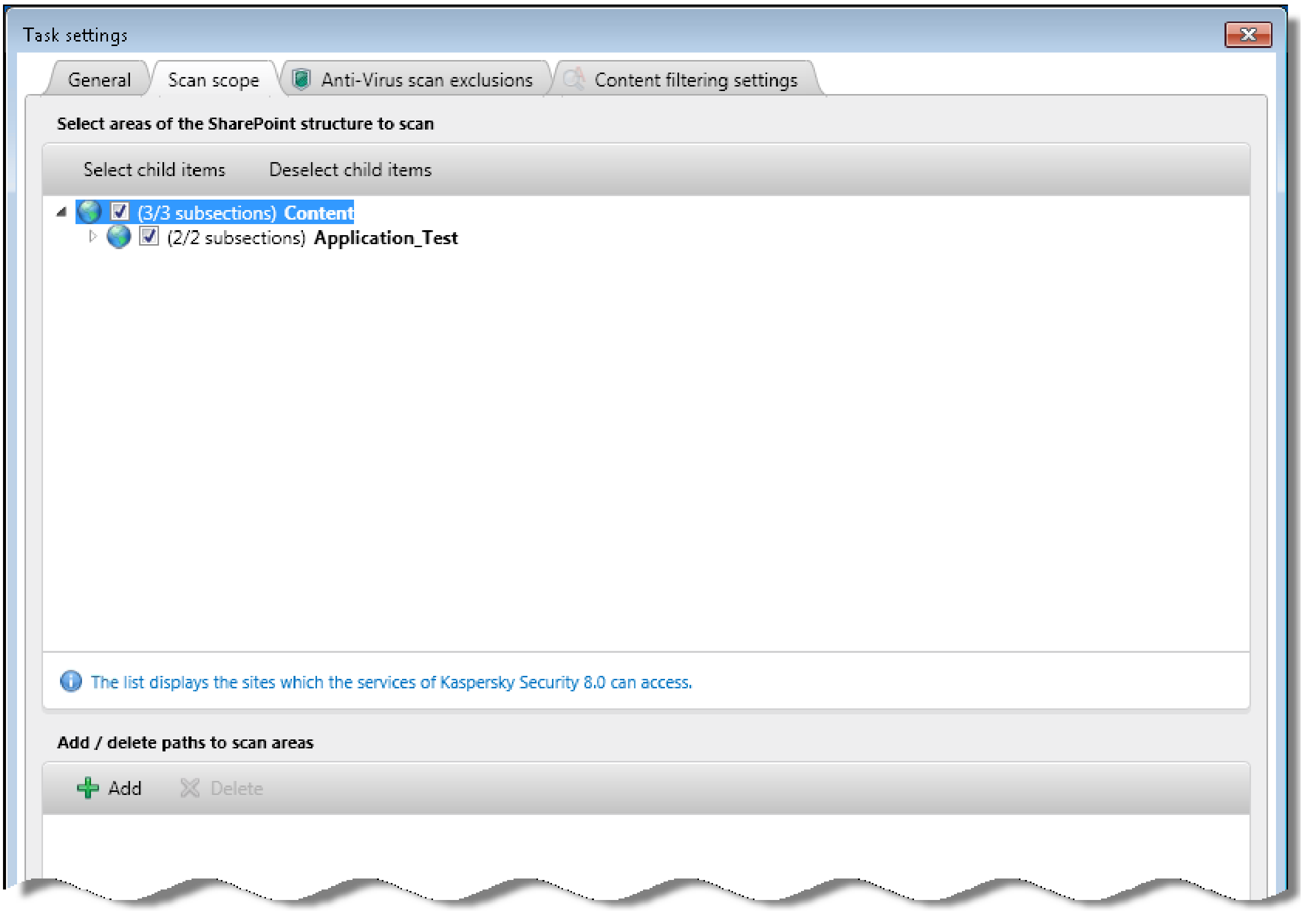
SELECTING AND EXCLUDING FROM ON-DEMAND SCANNING AREAS OF THE SHAREPOINT STRUCTURE

You can specify areas of the SharePoint structure to be scanned during an on-demand scan task. You can also exclude individual areas of the SharePoint structure from scanning.

➧ *To define the scan scope in a SharePoint structure:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Choose in the list of tasks displayed in the details pane the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Scan scope** tab (see the figure below).



Select areas of the SharePoint structure to scan

☑ (3/3 subsections) Content

☑ (2/2 subsections) Application_Test

The list displays the sites which the services of Kaspersky Security 8.0 can access.

Add / delete paths to scan areas

Figure 11: Selecting the scan area

3. Specify the scan area in the SharePoint structure in one of the following ways:

- In the SharePoint server structure tree, select check boxes corresponding to the SharePoint structure areas that you want to include in the scan scope. All check boxes are selected by default (all available SharePoint structure areas are scanned during the on-demand scan task).

> The tree only displays the SharePoint structure areas, for which administrator access is allowed to the account used to start the application services.

- Add SharePoint structure areas manually. To do so, perform the following in the **Adding / removing paths to scan areas** section:

a. Click the **Add** button. In the window that opens, enter the path to the area being added and click **OK**.

The following types of paths are supported:

- http://<SharePoint portal name>.local/content/;
- https://<SharePoint portal name>.local:8080/content/file.txt;
- http://<SharePoint portal name>/.

To remove an area, select it in the list and click **Delete**.

   a. Select the check box opposite the path to a SharePoint structure area, and select **Include** in the drop-down list.

   b. Clear the check box opposite the path to a SharePoint structure area, and select **Exclude** in the drop-down list.

4. Click **OK** to save changes and close the window.

➧ *To exclude SharePoint structure areas from an on-demand scan:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Choose in the list of tasks displayed in the details pane the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Scan scope** tab.

3. Exclude a SharePoint structure area from scanning in one of the following ways:

   - In the SharePoint server structure tree, clear the check boxes corresponding to the areas which you want to exclude from the scan scope.

   - In the **Adding / removing paths to scan areas** section, select **Exclude** in drop-down lists for the areas that you want to exclude from scanning.

4. Click **OK** to save changes and close the window.

CREATING ON-DEMAND ANTI-VIRUS SCAN EXCLUSIONS

To ease the load on the SharePoint server, you can exclude from the scope of on-demand Anti-Virus scanning specific formats or file name masks, restrict scanning duration for individual files.

➧ *To exclude specific file formats from on-demand anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Choose in the list of tasks displayed in the details pane the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Anti-Virus scan exclusions** tab.

3. In the **Exclude following file formats from scanning** list, select check boxes next to the file formats to be excluded from the scan scope (see the figure below).

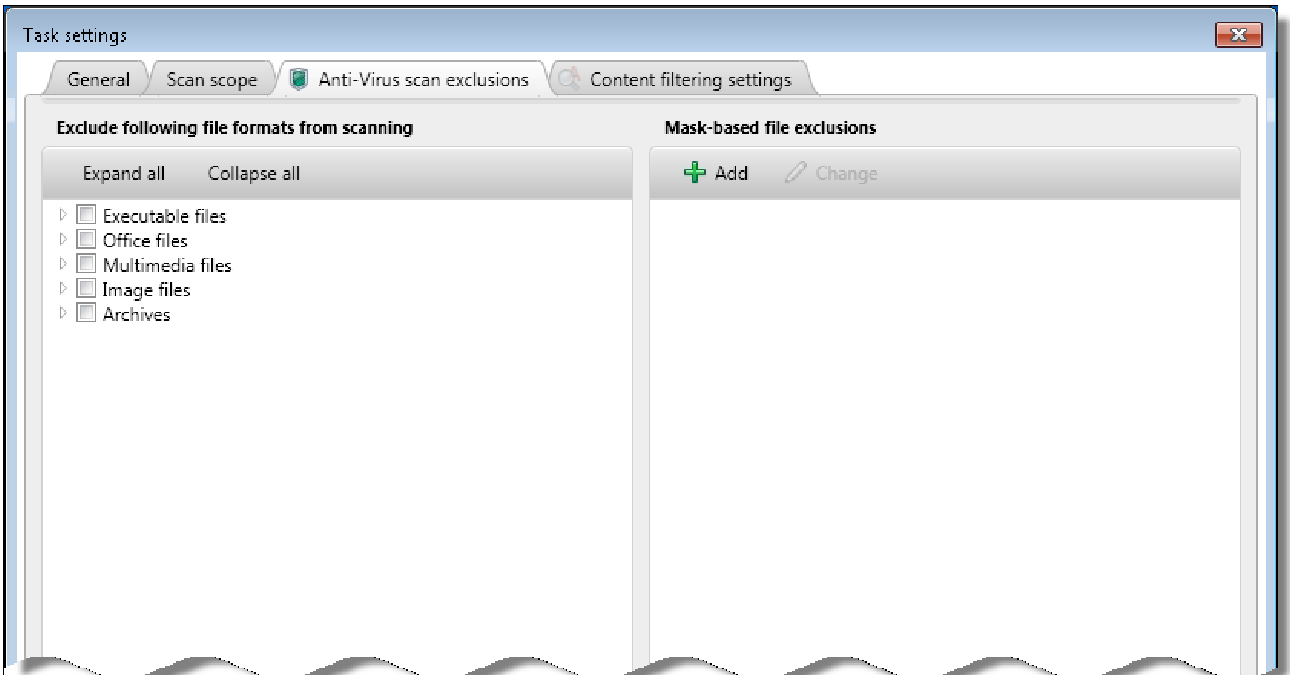


Figure 12: On-demand scan file exclusions

The tree can be managed conveniently using the **Expand all** and **Collapse all** buttons.

4. To save the changes and close the window, click **OK**.

➡ *To exclude files that match specific masks from on-demand Anti-Virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.
2. Choose in the list of tasks displayed in the details pane the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Anti-Virus scan exclusions** tab.
3. In the **Mask-based file exclusions** list, select check boxes next to file name masks to be excluded from the scan scope.
4. To add a mask to the list, click **Add** to open the **Add file mask** dialog and enter the mask in the entry field (see section "File name mask creation rules" on page 67). To save the changes and close the window, click **OK**.

   If you want to define several masks at once, use a semicolon as a separator.
5. To save the changes and close the window, click **OK**.

CONFIGURING CONTENT FILTERING

For on-demand scan tasks, you can configure the application to look for specific file formats, file name masks, and the categories of unwanted words and phrases.

➧ *To configure Content filtering in an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Choose in the list of tasks displayed in the details pane the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Content filtering settings** tab.

3. Configure the following Content filtering settings:

   - In the **Lists of categories**, select the check boxes next to the categories of Kaspersky Lab and user categories, which the application should seek while running the on-demand scan task.

   - In the **Unwanted file formats** list, select check boxes next to the file formats that should be scanned. To expand / collapse the entire list of formats and extensions, use the **Expand all** and **Collapse all** button.

   - In the **Sets of unwanted file name masks** list, select check boxes next to the sets of file name masks to be scanned during on-demand scanning.

4. To save the changes and close the window, click **OK**.

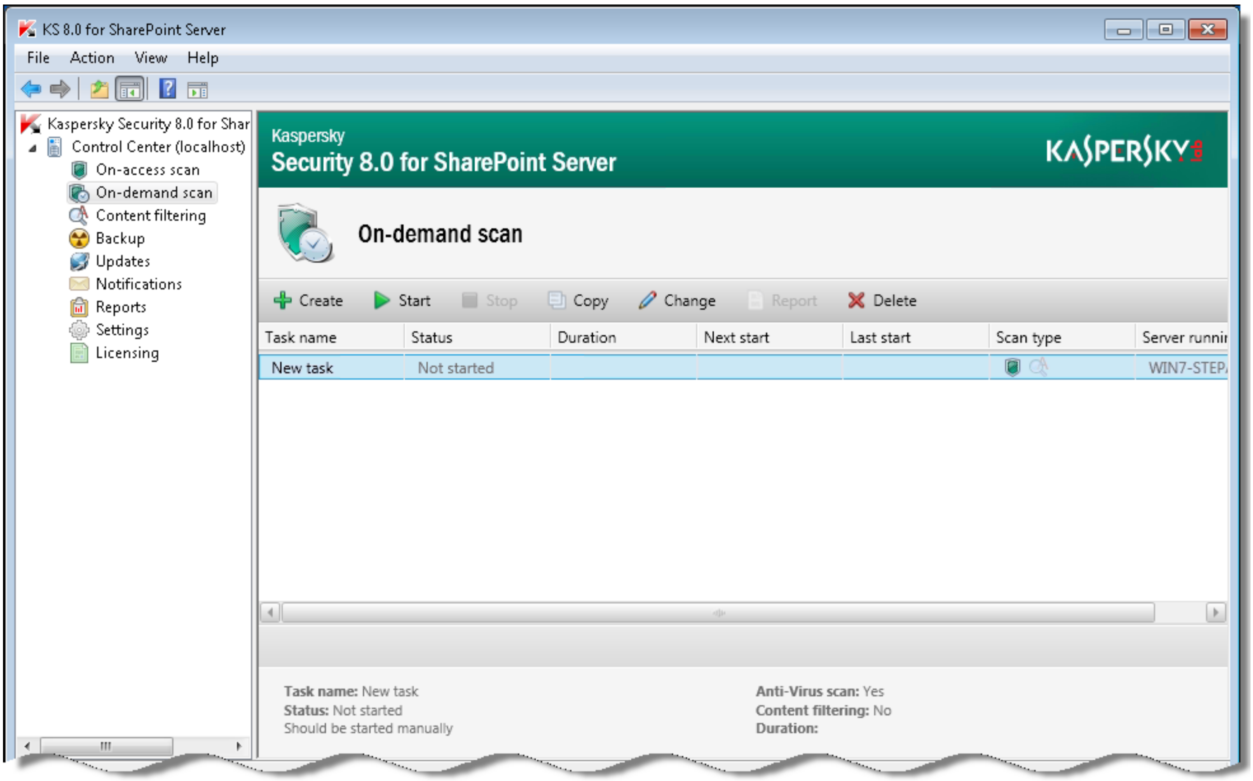
You can specify the file formats and file name masks and the composition of categories of unwanted words and phrases in the **Content filtering** node.

STARTING AND STOPPING ON-DEMAND SCAN TASKS

➧ *To start an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Select the on-demand scan task from the list in the details pane (see the figure below).



Task name	Status	Duration	Next start	Last start	Scan type	Server runnir
New task	Not started					WIN7-STEP.

Task name: New task
Status: Not started
Should be started manually

Anti-Virus scan: Yes
Content filtering: No
Duration:

Figure 13: Managing an On-demand scan task

3. Click the **Start** button to launch the on-demand scan task, or the **Stop** button to stop the task.

VIEWING AN ON-DEMAND SCAN TASK REPORT

➧ *To view a report on the results of an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Choose a task from the list in the details pane.

3. Click the **Report** button.

   The report is displayed in a new window of your web browser.

> The **Report** button is not available for tasks currently in progress and for tasks that have never been started.

The report contains the following information on the last on-demand scan:

- **Used task settings**:
  - task name;
  - task launch method (manual or scheduled);
  - scan task start and end times;
  - information about enabled application components;

  - name of the SharePoint where the task was performed;
  - task status;
- **Checking result**. Summarized information about the results of the on-demand scan task.
  - **Files skipped**. The number of files skipped by the application because of scanning errors.
  - **Scanned items**. Total number of scanned files.
  - **Virus threats found**. The number of malicious objects detected (the number Anti-Virus component incidents).
  - **Content filtering component positives**. Number of detected files in an unwanted format and file names containing unwanted masks, as well as web objects with unwanted content (number Content filtering incidents).
- **Table of positives**. A table with information about all files found to contain malicious objects or violations of Content filtering policies. If the scan has not detected any virus threats or violations of Content filtering policies, the *File scan detected no incidents* message is displayed instead of the table of positives.
  - **File name**. The name and path to the file where malicious objects or violations of content filtering policies have been found.
  - **Version**. File version on the SharePoint server.
  - **Action**. Operation performed on the file based on the scan results in accordance with the defined settings.
  - **Anti-virus scan**. Status assigned to the file by the anti-virus scanning component. This column shows the *Corrupted* or *Password protected* status label for corrupted or password-protected files. This column shows the name of the object detected in the file for infected or probably infected files.
  - **Content filtering**. Status assigned to the file by the Content filtering component. Violated policies that which triggered the Content filtering component.
  - **Backup**. Information about creation of a backup copy for the file in Backup.
  - **Restored version**. The version to be assigned to the restored file (if it can be disinfected).
  - **Incident ID**. The universal ID of the positive. The incident ID simplifies the search for information about the incident in the report, Backup, and file log. It is also displayed in the properties of a backup copy of the file in Backup and in notifications about violations of security policies during on-demand scanning.
- **SharePoint web objects scan alarms**. A table with the details of SharePoint web objects found to contain unwanted words or phrases. If no unwanted words or phrases have been detected during a scan of SharePoint web objects, the *SharePoint web objects scan detected no incidents* message is displayed instead of this table.
  - **Name and version**. Name and version of a SharePoint web object found to contain unwanted words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the Content filtering settings. The name consists of: <Site name> / <List name> / <Object ID>. The field contains n/a if the version information of the scanned SharePoint web object is unavailable.
  - **Categories**. List of SharePoint web object fields found to contain unwanted words or phrases, and categories to which the detected words and phrases belong.
  - **Incident ID**. The universal ID of the positive. The incident ID simplifies the search for information about the incident in the report and log file.
- **Scan area**. The list of all scan areas specified in the on-demand scan task settings.

DELETING AN ON-DEMAND SCAN TASK

➧ *To delete an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. Select in the details pane the task that you want to remove and click **Delete**.

CONTENT FILTERING

This section contains information about Content filtering and how to configure it.

IN THIS SECTION:

ABOUT CONTENT FILTERING

Kaspersky Security performs content filtering of files placed on the SharePoint server during on-access scanning (see section "On-access scan" on page 38) and on-demand scanning (see section "On-demand scan" on page 50).

Content is filtered by:

- file format
- file name mask You can specify masks for unwanted file names and formats.
- By the text content and names of the files. Kaspersky Security includes a preset collection of categories of unwanted words and phrases created by the experts at Kaspersky Lab. The collection is regularly updated from the servers of Kaspersky Lab. The preset collection of unwanted words and phrases cannot be modified. The window for adding new user categories of words and phrases.

> In case of integration with Microsoft SharePoint Server 2007 SP2 installed in Windows 2003 Server SP2, Kaspersky Security extracts and scans the content of text and RTF files only if the Windows Search 4.0 is installed in the host system.

File content is scanned using the libraries of filters via the IPersistStream interface. To enable or disable filters available on a server, you can use Kaspersky IFilter Utility, which is installed together with Kaspersky Security.

More details about IFilter can be found at http://msdn.microsoft.com/en-us/library/ms691105%28v=vs.85%29.aspx.

When the application is installed, filters included in following standard filter packs are enabled by default:

- Windows Server (installed with the operating system).
- SharePoint (installed with the SharePoint server).
- Office 2007 Filter Pack
- Office 2010 Filter Pack

If other filters are installed on the SharePoint server, they are disabled by default and content filtering by format is not performed for files scanned using these filters. Use Kaspersky IFilter Utility to enable such filters.

You can enable / disable the installed filters and also install necessary additional filters using utility.

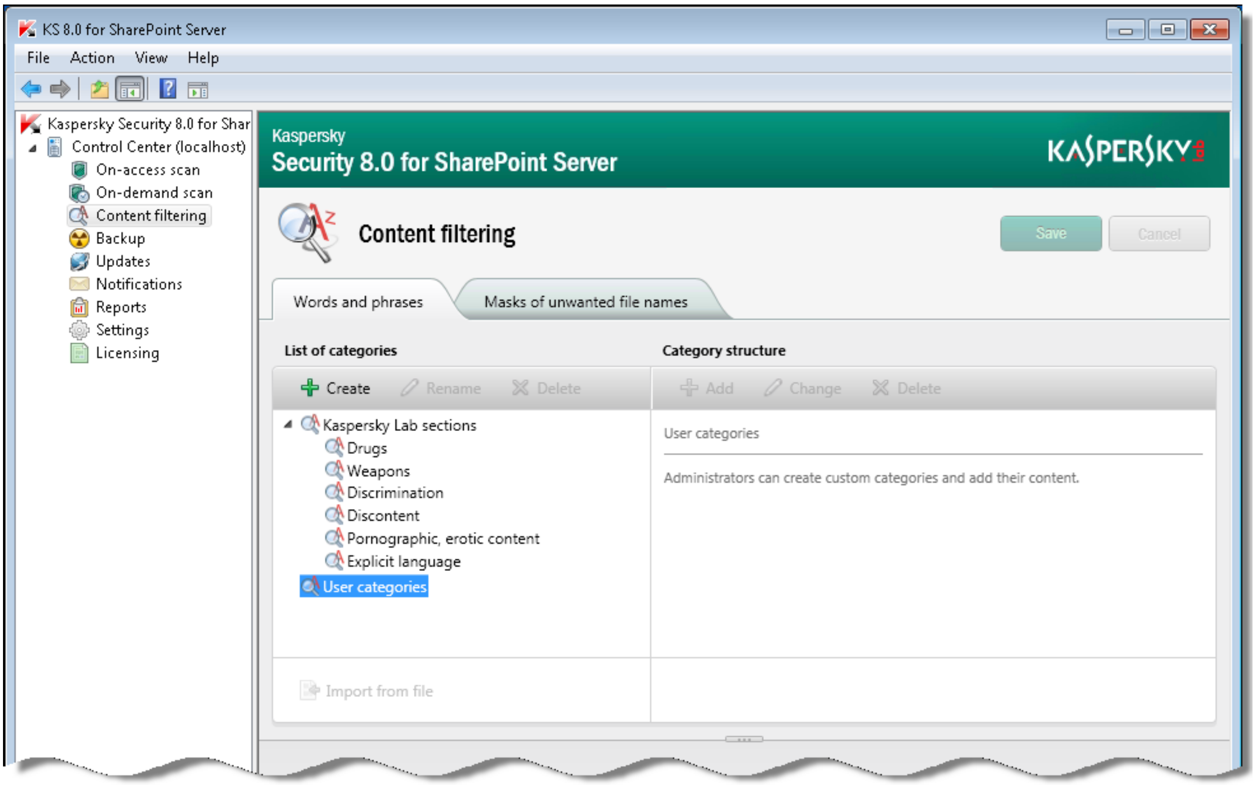
You can start the utility from the menu **Start** □ **Programs** □ **Kaspersky Security 8.0 for SharePoint Server** □**Kaspersky IFilter Utility**.

For more details on the Kaspersky IFilter Utility, please refer to the online Help file.

CREATING, RENAMING, AND DELETING USER CATEGORIES OF UNWANTED WORDS AND PHRASES

To create a new user category of unwanted words and phrases:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node (see the figure below).



Administrators can create custom categories and add their content.

*Figure 14: **Content filtering** node*

2. In the details pane, select the **Words and phrases** tab and click the **Create** button in the **List of categories** section.

3. Enter the name for the new category in the displayed **Add category** dialog.

4. Click **OK**.

To rename a user category of unwanted words and phrases:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the **Words and phrases** tab, select the category that you want to rename and click **Rename**.

3. Enter the new name for the category in the displayed **Category editing** dialog and click **OK**.

To delete a category for unwanted words and phrases:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the **Words and phrases** tab, on the **List of categories** section select the category that you want to delete and click **Delete**. Selected category will be removed from the list.

> Only user categories can be created, renamed or deleted. You cannot change the preset collection of Kaspersky Lab categories included in the application.

RULES FOR USING CHARACTERS IN USER CATEGORIES

The following characters and punctuation marks are ignored in word and phrase searches:

- Punctuation marks: comma (html-code 44), period (html-code 46), colon (html-code 58), semicolon (html-code 59), single and double quotes (html-codes 39 and 34), angular brackets (html-codes 171 and 187), hyphen (html-code 45), short and long dash (html-codes 8211 and 8212), ellipsis (html-code 8230), round brackets (html-codes 40 and 41), square brackets (html-codes 91 and 93), curved brackets (html-codes 123 and 125), angular brackets (html-codes 60 and 62), slash (html-code 47).

- Characters: reverse slash (html-code 92), degree mark ° (html-code 176), ® (html-code 174), ¦ (html-code 166), ™ (html-code 8482), √ (html-code 8730), © (html-code 169), № (html-code 8470).

The following characters are forbidden: • (html-code 149) and ‼ (html-code 8252).

ADDING, CHANGING, AND DELETING UNWANTED WORDS AND PHRASES IN USER CATEGORIES

To add an unwanted word or phrase to a user category:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the tab **Words and phrases** and pick in the **List of categories** the custom category, where you want to add a word or phrase.

3. In the **Category structure** field, click **Add**. Type the word or phrase in the field within the displayed dialog.

> Refer to the rules for using characters in words and phrases (see section "Rules for using characters in user categories" on page 64).

4. If you want the application to consider case while searching for a word or phrase, select the check box **Case-sensitive**. Click **OK**.

> You can specify several words or phrases. Use the "|" character as a delimiter.

➧ *To edit a word or phrase within a selected user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the results pane, select the tab **Words and phrases** and pick in the **List of categories** the custom category containing the word or phrase that you want to edit.
3. Select in the **Category structure** field the word or phrase, which you want to change and click **Change**.
4. Edit the word or phrase in the displayed window. Select the **Case-sensitive** check box as required. Click **OK**.

➧ *To delete a word or phrase from a selected user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the results pane, select the tab **Words and phrases** and pick in the **List of categories** the custom category containing the word or phrase that you want to delete.

> You can select several words of phrases in the list while holding the **SHIFT** key pressed.

3. Select in the **Category structure** field the word or phrase, which you want to delete and click **Delete**.

> Only user categories can be created, edited or deleted. You cannot change the preset collection of Kaspersky Lab categories included in the application.

IMPORTING A LIST OF UNWANTED WORDS AND PHRASES INTO A USER CATEGORY FROM A TEXT FILE

You can import from a text file a list of unwanted words and phrases into a user category.

The words and phrases in such file must comply with the following conditions:

- Each line must contain just one term with its word forms.
- The term should be separated from its word forms with the "|" character.
- Term length may not exceed 127 characters.

> If a term contains special symbols or multibyte characters, for example, UTF-8 (encoded using three or more bytes), the term length must not exceed 64 characters.

➡ *To import a list of unwanted words and phrases into a user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the results pane, select the **Words and phrases** tab and in the **List of categories** field select the category that you want to import the list into.
3. In the **List of categories** field, click the **Import from file** button. In the displayed window specify the path to the necessary file.

   > The **Import from file** button is only available for the user-defined categories of unwanted words and phrases.

4. To save the changes, click **Save**.

ABOUT THE WHITE LIST

The while list is a list of words and / or phrases that should be skipped by Content filtering.

The white list contains words and / or phrases that, although included in prohibited categories of Kaspersky Lab, should be skipped by Content filtering. By using the white list, it is possible to avoid false positives of the application component on detecting words and / or phrases that are permissible in and specific to the field of the company's business.

The white list is local. It is created separately for each farm server. When a word and / or phrase is included in the white list, all of its word forms should be specified for the application component to work properly.

Example:

<string>sea</string>

<string>seas</string>

<string>seaside</string>

<string>seasick</string>

Changes made to the list are applied with a delay of no more than 5 seconds.

CREATING THE WHITE LIST

➡ *To create a white list of permissible words and / or phrases:*

1. Open the folder with SharePoint server configuration files by performing the following:
   - If the application is installed on a farm of SharePoint servers, open the application setup folder and go to the folder of the corresponding farm server. Then open the **Configurations** folder.
   - If the application is installed on a standalone SharePoint server, open the application setup folder and go to the **Configuration** folder.
2. Create an XML file with the name ContentFilteringWhitelist.

   The ContentFilteringWhitelist.config file must have the following structure:

   <?xml version="1.0" encoding="utf-16"?>

   <configuration version="1.0">

```
<ContentFilteringWhitelistSubset ContentxmIns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Items>

<string></string>

</Items>

</ContentFilteringWhitelistSubset>

</configuration>
```

3. Type the word or phrase to be skipped by Content filtering between the <string> and </string> tags.

   Type each new word or phrase and their word forms in a new line between the <string> and </string> tags.

4. Save changes to the file in Unicode format.

If you save the file in a different format, the words and / or phrases typed using a Cyrillic font may be displayed incorrectly in the error log.

File name mask creation rules

Please follow these guidelines on creating masks:

- The following wildcards are supported:
  - * – an arbitrary string of characters. For example, the "abc*" mask stands for any file with the name beginning with the "abc" string: abc.exe, abc1.com, abc2.rar.
  - ? – any single character. For example, the "abc?.exe" mask stands for any file with the name beginning with the "abc" string followed with an arbitrary single character, like abc1.exe. However, the file abc12345.exe will not match the mask.
- Observe the following restrictions:
  - Masks cannot contain the following characters: >, <, \, /, |, ", ;.
  - It is not recommended to use masks that match the file extensions of SharePoint service files (for example, *.aspx, *.html, *.mht) in the content filtering settings. Deleting SharePoint service files could disrupt the operation of SharePoint.

CREATING, RENAMING, AND DELETING A SET OF MASKS FOR UNWANTED FILE NAMES

To create a new set of forbidden file name masks:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node (see the figure below).

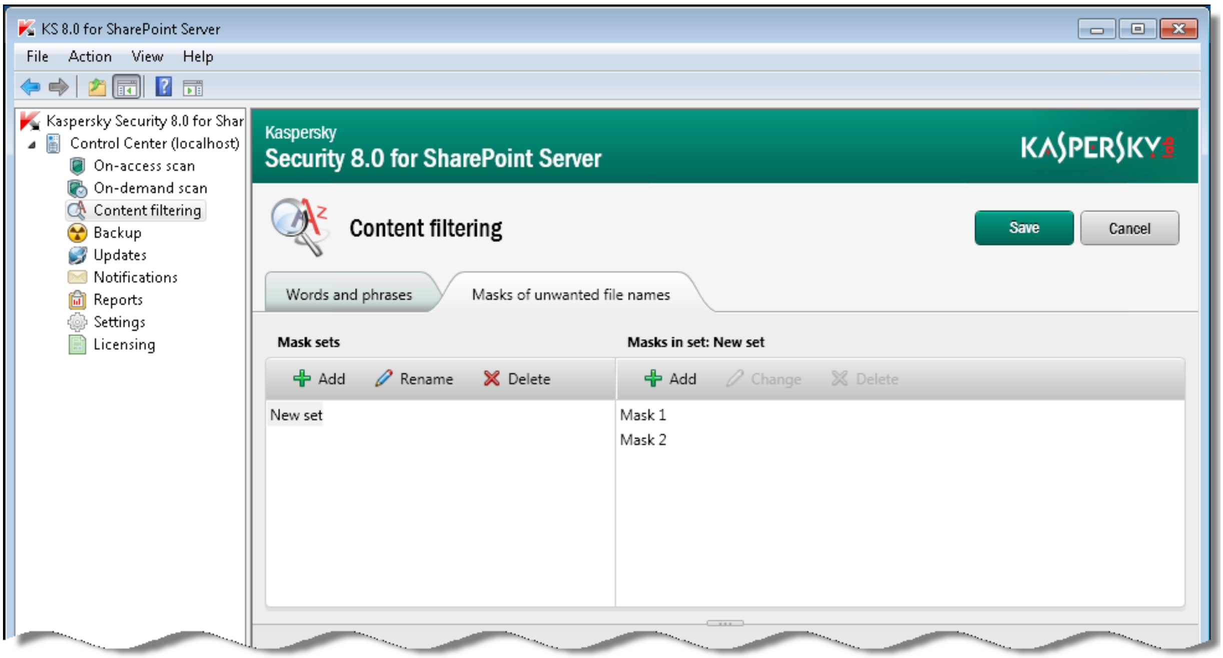


Figure 15: ***Masks of unwanted file names*** *tab*

2. In the details pane, on the **Masks of unwanted file names** tab and click **Add.** The **Add name of a set of file masks** dialog will appear
3. Enter in the displayed dialog the name for the new set of masks.
4. Click **OK**.

To rename a set of masks for unwanted file names:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the results pane, on the **Masks of unwanted file names** tab , select the set that you want to rename, and click **Rename**.
3. Enter the new name for the mask set in the displayed dialog and click **OK**.

To delete a set of unwanted file name masks:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the results pane, on the tab **Masks of unwanted file names,** select the mask set that you want to delete, and click **Delete**.

CHANGING A SET OF UNWANTED FILE NAME MASKS

➧ *To add an unwanted file name mask to a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the tab **Masks of unwanted file names** and in the **Mask sets** field pick the set where you want to add a mask (see the figure below).

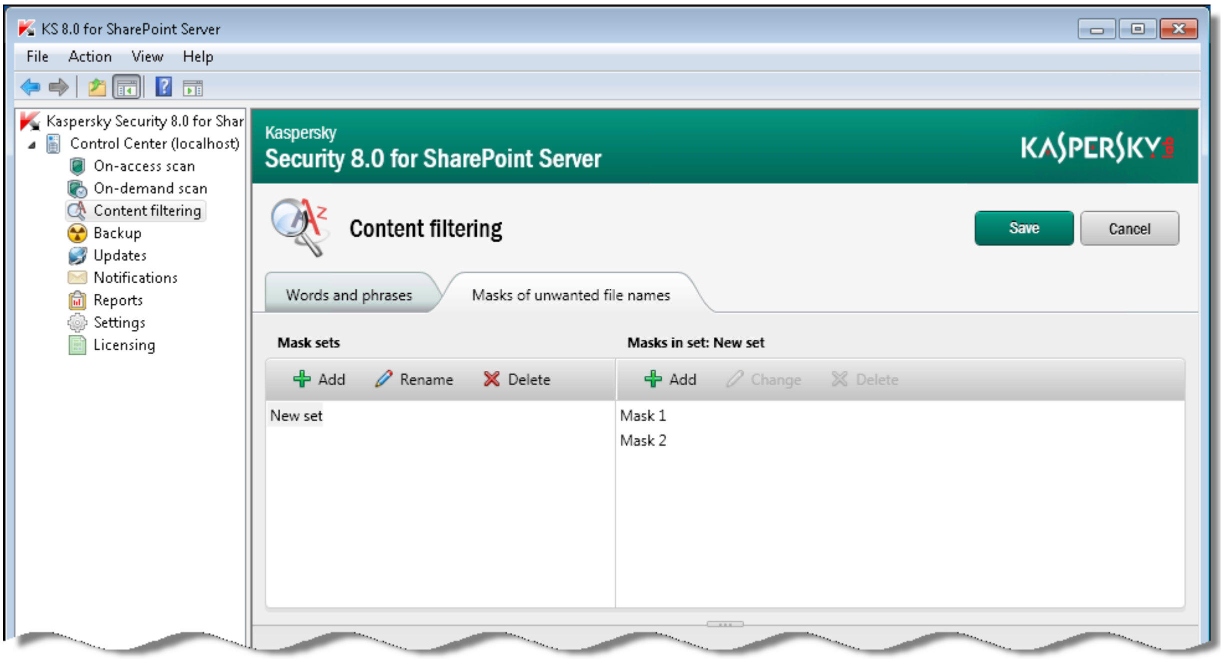


*Figure 16: **Masks of unwanted file names** tab*

3. In the **Masks in set** field, click the **Add** button. In the window that opens, specify the mask of the unwanted file name in the field.

> You can specify several masks. Use a semicolon as a delimiter.

➧ *To edit the unwanted file name masks in a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the tab **Masks of unwanted file names** and in the **Mask sets** field pick the set containing the masks which you want to edit.

3. In the **Masks in set** field select the mask that you want to edit and click **Edit**.

4. Edit the mask in the displayed window and click **OK**.

➧ *To delete an unwanted file name mask from a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the results pane, select the tab **Masks of unwanted file names** and in the **Mask sets** field pick the set containing the masks which you want to delete.

> You can select several masks in the set while holding the **SHIFT** key pressed.

3. In the **Masks in set** field select the mask that you want to delete and click **Delete**.

> If multiple masks have been selected within a set, you can only delete the selected masks. No other operations with them will be available.

ABOUT THE LOG OF CONTENT FILTERING INCIDENTS

The log of Content filtering incidents lets you check if the Content filtering settings are properly configured.

The log of Content filtering incidents is located in the folder <Application setup folder>\logs\content_filtering\content_filtering_incidents_log_YYYYDDMM.csv, where YYYYDDMM stands for the log creation date.

> The log of Content filtering incidents is created on a daily basis and contains the details of content filtering incidents for the relevant day. Logs for the previous days are stored in the folder <Application setup folder>\logs\content_filtering in archives with the corresponding names.

When a Content filtering incident is caused by the name or content of a file, the following details are recorded in the log of content filtering incidents:

- Incident ID
- Path to file
- File name
- The word or phrase that caused the Content filtering incident
- The Kaspersky Lab section or user category to which the specific word belongs

When a Content filtering incident is caused by the content of a SharePoint web object, the following details are recorded in the log of Content filtering incidents:

- Incident ID
- Path to the SharePoint web object
- Name of the field of the SharePoint web object in which unwanted content has been detected
- The word that caused the Content filtering incident
- The Kaspersky Lab section or user category to which the specific word belongs

To perform a more detailed check the operation of Content filtering, you can enable the detailed log of Content filtering incidents (see section "Keeping a detailed log of content filtering incidents" on page 70).

KEEPING A DETAILED LOG OF CONTENT FILTERING INCIDENTS

To check the operation of Content filtering, you can enable the detailed log of Content filtering incidents.

➡ *To enable the detailed log of Content filtering incidents:*

1. Select and open in the console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.

2. In the **Diagnostics** configuration section, select the **Enable detailed log of Content filtering incidents** check box.

   The log of Content filtering incidents will additionally record the sequence of characters from the text extracted from the file or the field of a SharePoint web object by the corresponding filter of Kaspersky IFilter Utility.

   > The log records a sequence of 10 words located in the text before the word that caused the content filtering incident, the word itself, and 10 words located in the text after the word that caused the Content filtering incident. If these 10 words contain more than 100 characters, the sequence is limited to 100 characters before and after the word that caused the Content filtering incident.

3. To save the changes, click the **Save** button in the upper part of the window.

BACKUP

This section contains information about the Backup, describes its configuration and management of document copies stored in Backup.

IN THIS SECTION:

ABOUT BACKUP

Kaspersky Security saves in Backup copies of files that require action based on the results of Anti-Virus scanning and / or Content filtering (such as blocking or deletion). The application places in Backup copies of all harmful files, whether they can be disinfected or not.

Kaspersky Security places files to the Backup storage in encrypted form, which prevents the infection risk (files in Backup storage are not accessible without decryption).

Backup size

The data volume that can be stored in the Backup may be restricted by one of the two following parameters:

- Total number of files in Backup cannot exceed 50000. You cannot remove or change this restriction.
- The default size of Backup is 3686 MB. You can change the size of Backup (see section "Configuring automatic Backup purging" on page 97).

Deleting files from Backup

The application periodically (every time a new file is placed in Backup) checks compliance with the set restrictions on the size of Backup.

If the restrictions are exceeded, the application:

- Stops placing files in Backup, if the number of files in storage is exceeded.
- Frees up the necessary disk space by deleting the oldest files, if the restriction on storage size is exceeded by the addition of another file. The files stored for the longest amount of time are deleted first.

You can also delete files from Backup manually. For example, you may need to delete files that have been successfully restored after disinfection, or delete all files to purge Backup.

OPERATIONS WITH OBJECTS PLACED IN BACKUP

You can perform the following actions on objects stored in Backup:

- View a list of files with detailed information about files placed in Backup in table form;
- Use the quick search function or extended filter to find the files in the list;

- Restore files, for example, if you want the application to rescan them using an updated version of the databases;
- Save files to the local drive on your computer, for example, to inspect them more closely;
- Delete files from Backup that are no longer needed;
- Purge Backup by deleting all files from it.

IN THIS SECTION:

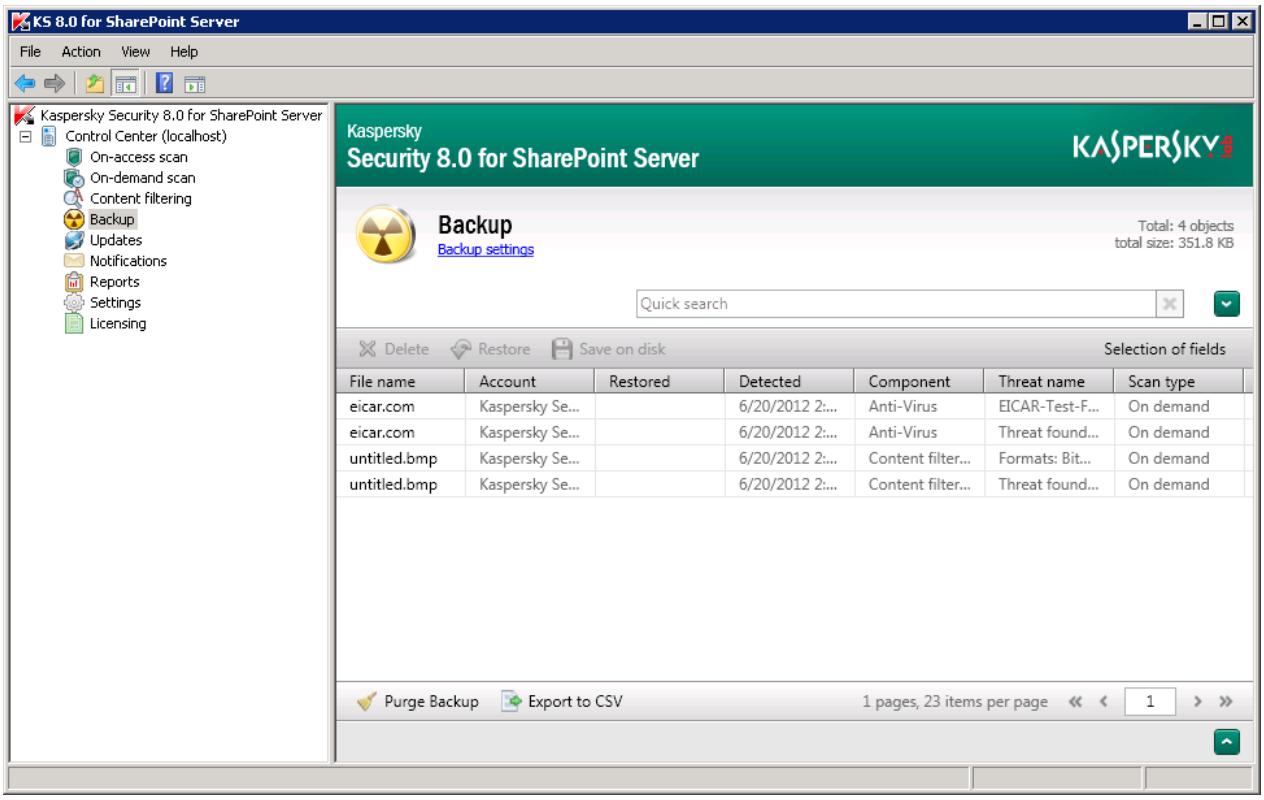
VIEWING THE LIST OF FILES IN BACKUP

You can view the list of files in Backup; it is displayed as a table with corresponding column headers.

➧ *To view the list of files in Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

The results window will display information about Backup and the list of files inside (see the figure below).



Total: 4 objects
total size: 351.8 KB

File name	Account	Restored	Detected	Component	Threat name	Scan type
eicar.com	Kaspersky Se...		6/20/2012 2:...	Anti-Virus	EICAR-Test-F...	On demand
eicar.com	Kaspersky Se...		6/20/2012 2:...	Anti-Virus	Threat found...	On demand
untitled.bmp	Kaspersky Se...		6/20/2012 2:...	Content filter...	Formats: Bit...	On demand
untitled.bmp	Kaspersky Se...		6/20/2012 2:...	Content filter...	Threat found...	On demand

Figure 17: Backup

The top right corner of the details pane displays the number of files placed in Backup and the total size of these files.

The bottom right corner of the details pane displays the following information:

- The range of lines in the table listing files.
- The number of lines in the table listing files.
- The page number of the files list.

In the files list you can view the information about files stored in Backup. The appearance of the files list may differ depending on the columns selected for display.

By default, the list contains the following file information:

- **File name**. File name.
- **Path to file**. The path to the original location of the file on the server.
- **Account**. Account of the user who had performed the operation that resulted in file addition to Backup.
- **Restored**. Date and time of file restoration on server.
- **Detected**. Date and time of object detection in file.
- **Component**. The module, that scanned the file - anti-virus scan or content filtering.
- **Object name**. Name of the object detected in the file.

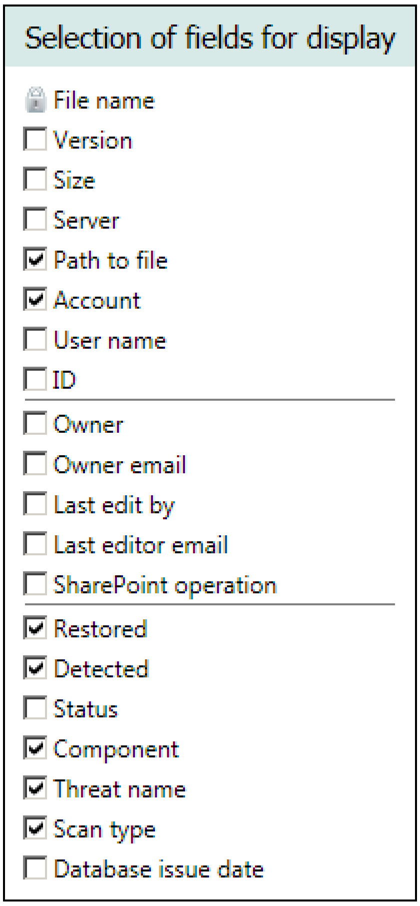
- **Scan type**. The type of scan which detected the object – on-demand or on-access scan.

> The columns **Path to file**, **Owner**, **Owner email**, **Last edit by** and **Last editor email** cannot be filled during on-access scanning while working with Microsoft SharePoint Server 2007 due to technical peculiarities of the server.

2. Configure the appearance of the files list (if necessary) by selecting the columns to be displayed in the table:

   a. Click **Selection of fields**.

   The **Select the fields to display** dialog will appear (see the figure below).



Selection of fields for display

🔒 File name
□ Version
□ Size
□ Server
☑ Path to file
☑ Account
□ User name
□ ID

□ Owner
□ Owner email
□ Last edit by
□ Last editor email
□ SharePoint operation

☑ Restored
☑ Detected
□ Status
☑ Component
☑ Threat name
☑ Scan type
□ Database issue date

Figure 18: Selecting file information fields to display

   The columns in the table of files will appear and disappear as you select or clear their corresponding check boxes.

> The **File name** column is always displayed. It cannot be hidden.

   b. Left-click with the mouse outside the **Selection of fields** area to close the window.

3. You can sort the files list in the table by any of the columns in ascending or descending order, as required. To do that, click the header of the column that you want to use to sort files, for example, **File name**, **Path to file**, **Component**. If you want to reverse the sorting order, click the header once again.

   The list of files will be sorted by the selected column. The sorting symbol will appear in the header of the selected column:

- ▾ – sorted in ascending order

- ▲ – sorted in descending order

To view the details of a specific file, select it in the file list using the buttons to navigate to the next / previous, first / last pages of the file list « ‹ 1 › ». To find files in the list, you can also use the quick search (see section "Searching files in Backup: quick search" on page 76) and extended filter functions (see section "Searching files in Backup: extended filter" on page 77).

SEARCHING FILES IN BACKUP: QUICK SEARCH

➧ *To quick-search files in Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The details pane will display the list of files stored in Backup.

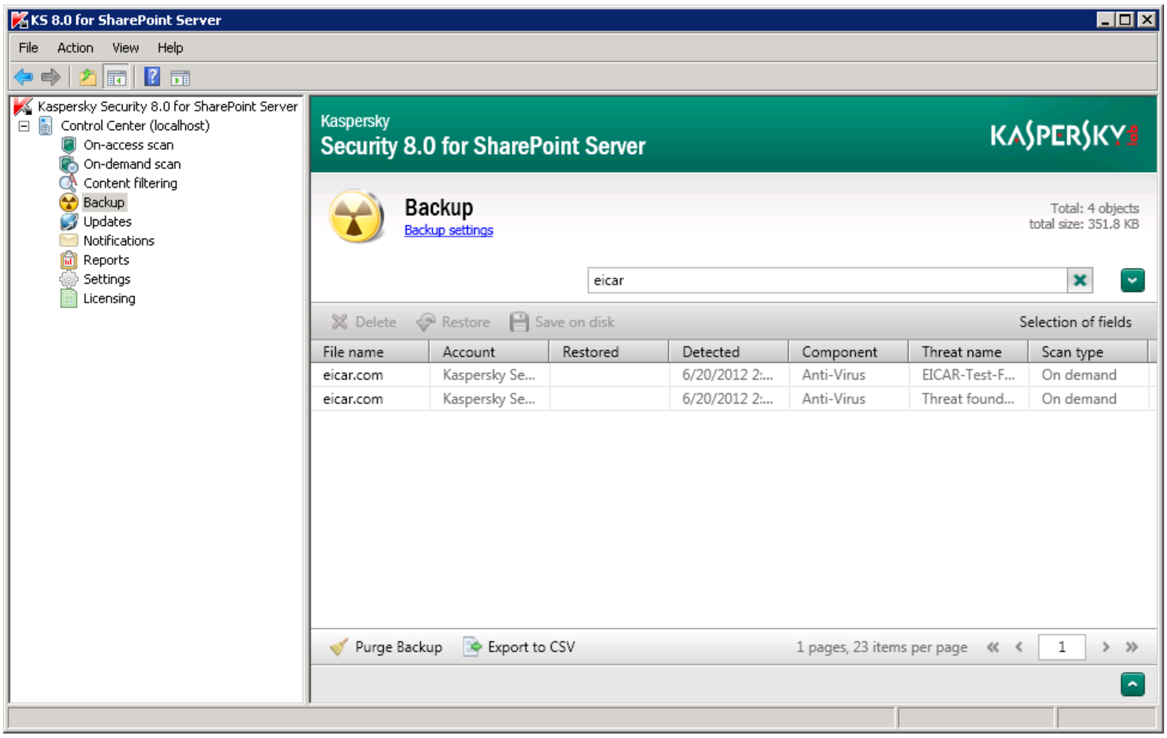
2. Enter the pattern string for file search in the **Quick search** field. The pattern string supports masks.

   Quick search begins acting immediately as soon as you enter the template string.

   The list of document copies will only display files matching the search condition (see the figure below). A file will match the search condition if the entered pattern string can be found in at least one of the following file properties:

   - **File name**.
   - **SharePoint server name**.
   - **Path to file**.
   - **User account**.
   - **User name**.
   - **Owner**.
   - **Last edit by**.
   - **Object name**.

- **Incident ID**.



File name	Account	Restored	Detected	Component	Threat name	Scan type
eicar.com	Kaspersky Se...		6/20/2012 2:...	Anti-Virus	EICAR-Test-F...	On demand
eicar.com	Kaspersky Se...		6/20/2012 2:...	Anti-Virus	Threat found...	On demand

Figure 19: Quick search in Backup

To cancel quick search, click the ✖ icon next to the **Quick search** field.

SEARCHING FILES IN BACKUP: EXTENDED FILTER

➨ *To find files in Backup using the extended filter:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. Click the ⌄ icon to maximize the extended filter section.

   The extended filter section will be displayed. The section contains the list of filter conditions. By default, the list contains three lines where you can specify the conditions that will be used to filter document copies. Each filter condition consists of three parts: the file property to check, the pattern string and the comparison rule applied while matching the property and the pattern string.

3. To define a filtration condition:

   a. Select the property to check from the drop-down list in the left part of the line.

      You can pick any of the following values as the property to check:

      - **File name**.
      - **SharePoint server name**.
      - **Path to file**.

- **User account**.
- **User name**.
- **Incident ID**.
- **Owner**.
- **Owner email**.
- **Last edit by**.
- **Last editor email**.
- **Object name**.

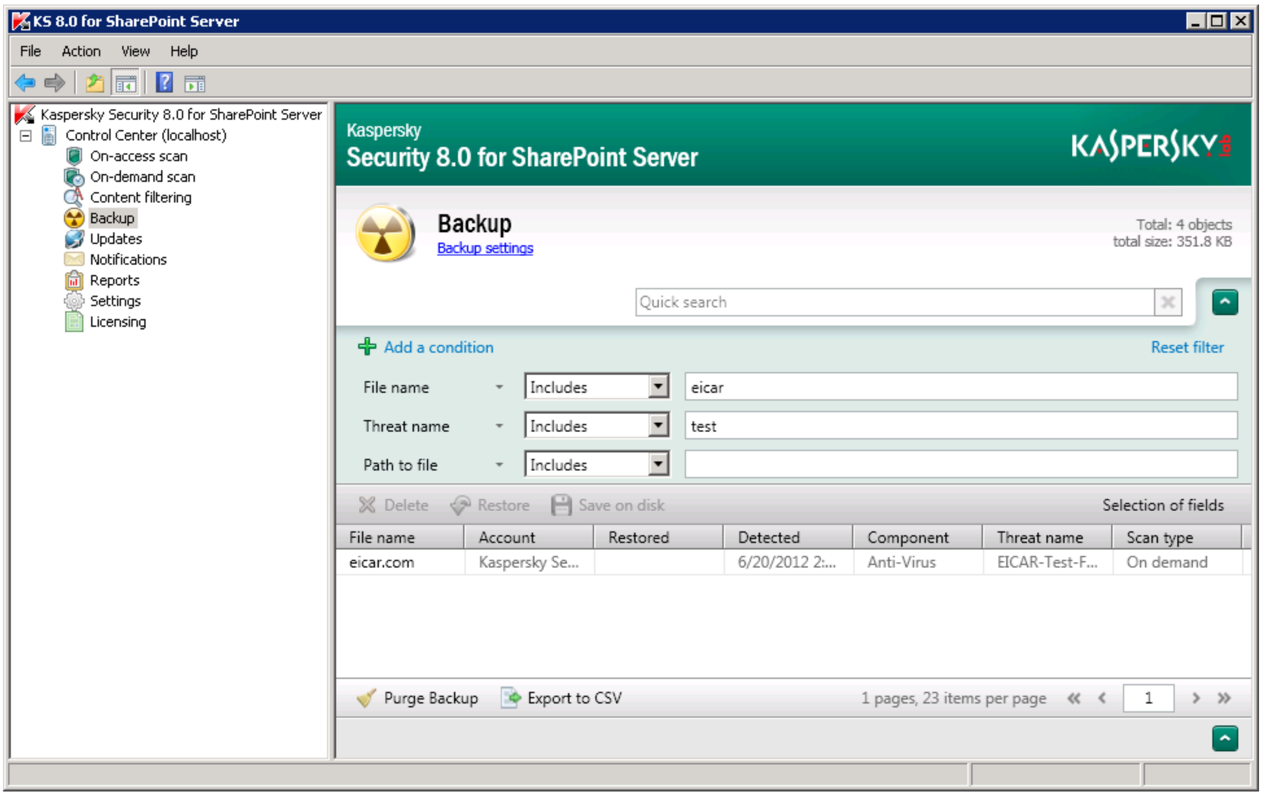
b. Select the comparison rule from the drop-down list in the middle of the line.

The set of values in the list will correspond to the selected value of the property to check. For example, for the **File name** property the list will offer the following values: **Includes**, **Does not include**, **Empty field**.

> If you have selected **Empty field**, the text input box in the right part of the line will become inactive.

c. Enter the template string in the entry field in the right part of the line. The pattern string supports masks.

Specified filter condition will be applied to the list of files in Backup immediately as soon as you specify all its three parts. The files list will only display files matching all specified filtering conditions (see the figure below).



Total: 4 objects
total size: 351.8 KB

File name	Includes	eicar
Threat name	Includes	test
Path to file	Includes	

File name	Account	Restored	Detected	Component	Threat name	Scan type
eicar.com	Kaspersky Se...		6/20/2012 2:...	Anti-Virus	EICAR-Test-F...	On demand

1 pages, 23 items per page 1

Figure 20: Using an extended filter

4. If you need to define more than three filter conditions, you can append additional lines to the list of conditions. To do that, click **Add a condition**.

A new line will appear in the lower part of the filter conditions section.

5. If you want to delete an additional filter condition, click the ✖ icon in the filtering condition line.

   The selected line will be deleted from the list of filter conditions. The list of files will be refreshed to match the remaining filter conditions.

For convenience you can minimize the extended filter section by clicking the ⌃ icon. Minimized extended filter will continue to function. If you want to cancel extended filtration, click the **Reset filter** link.

RESTORING FILES FROM BACKUP

➡ *To restore files from Backup:*

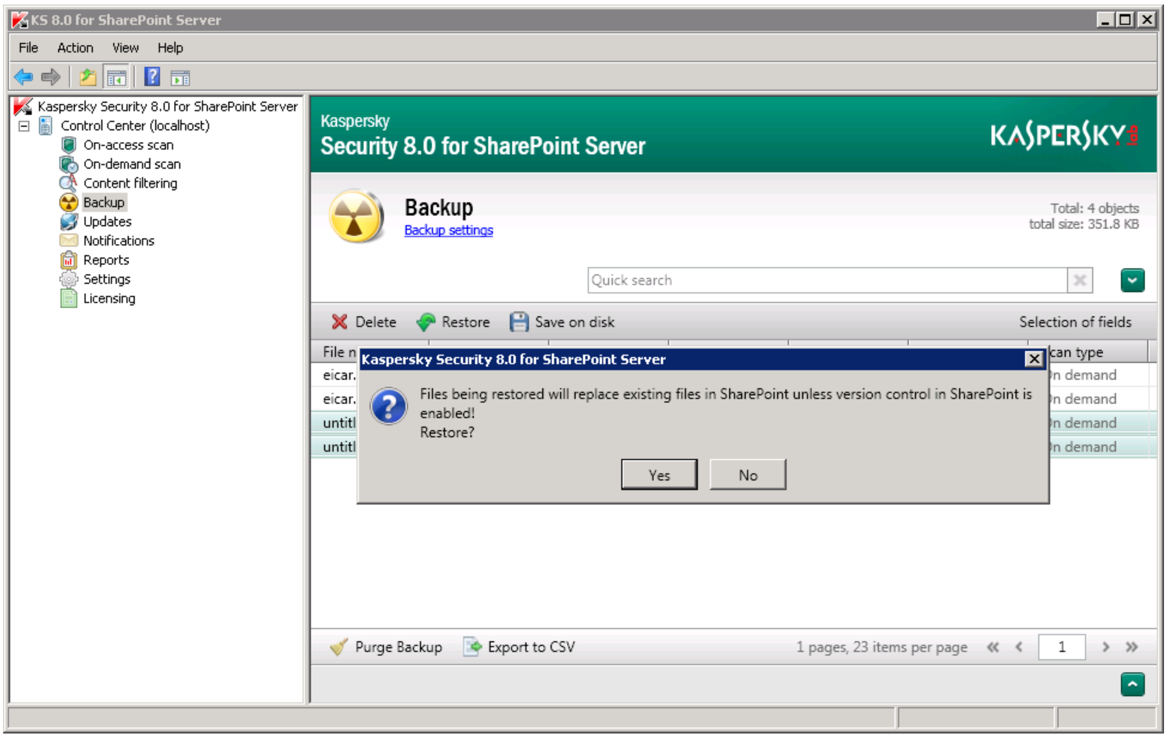
1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The details pane will display the list of files stored in Backup.

2. Select the files that you want to restore in the table.

   Restoring files containing viruses and malicious objects can cause the computer to be infected.

3. Click **Restore** (see the figure below).



Kaspersky Security 8.0 for SharePoint Server

Files being restored will replace existing files in SharePoint unless version control in SharePoint is enabled!
Restore?

Yes | No

Figure 21: Restoring files from Backup

Selected files will be decrypted and restored to the original locations in SharePoint structure. The files will be restored in the same format and under the same names they had when they were added to Backup.

While restoring objects, the application updates in SharePoint the following relevant information:

- **User**. The application records to the field the account name of its administrator.

- **Comments**. The application records in this field the application name, date when an object was placed in Backup and file version.
- **Version**. The application updates the file version.

After file restoration its copy and relevant information remains in Backup.

RULES FOR RESTORING FILES OF THE SAME NAME IN SHAREPOINT

When files are being restored from Backup, it is possible that the path specified in SharePoint points to a file of the same name. Restoration of files of the same name depends on version control settings configured on the SharePoint server.

The following version control options exist:

- *Major*. File versions are available to all users of the SharePoint server.
- *Minor*. File versions are available to a limited group of users.

Restoring a file of the same name with version control enabled

If there is no file of the same name in SharePoint, the application restores the object from Backup as a file with the first minor or major version, depending on the version of the file when a copy of it was placed in Backup. If major version control is enabled in SharePoint, the file will be restored as a file with the corresponding major version.

If there is a file of the same name in SharePoint, Kaspersky Security restores the file according to the following rules:

- Kaspersky Security restores the new minor version if minor/major version control is enabled in SharePoint and the file in Backup has a minor version.
- Kaspersky Security restores the new major version in all other cases.

If the file being restored has no version, the application restores the file as a file with a new minor version (if minor/major version control is enabled in SharePoint), or as a file with a new major version (if major version control is enabled).

Restoring a file of the same name with version control disabled

In this instance, Kaspersky Security prompts you to replace the file of the same name with the file being restored.

You can select one of the following actions in the window with the prompt to replace the file:

- **Yes**. The file in SharePoint is replaced with the file being restored.
- **No**. The file in SharePoint is not replaced with the file being restored. In this case, the file being restored remains in Backup.

When several files are being restored from Backup and there is a file of the same name of at least one of them in SharePoint, Kaspersky Security prompts you to replace the file / files of the same name with the file / files being restored.

You can select one of the following actions in the window with the prompt to replace the file / files:

- **Yes, restore the file**. The file in SharePoint will be replaced with the restored file.
- **No, do not restore the file**. The file in SharePoint will not be replaced with the restored file.

SAVING FILES IN BACKUP TO DISK

➧ *To save files in Backup to disk:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. If you want to save a single file to disk:

   a. Select in the files list the file, which you want to save to disk. You may use quick search or extended filter to find the file.

   b. Click the **Save** button.

      The standard file saving dialog will appear.

   c. Select the destination folder for the file.

   d. If you want to save the file under a different name, enter it in the **File name** field.

   e. Click the **Save** button.

      Selected file will be saved in the destination folder.

3. If you want to several files to disk:

   a. Select in the list the files, which you want to save to disk. You may use quick search or extended filter to find the files.

   b. Click the **Save** button.

      The standard destination selection dialog will appear.

c. Select the destination folder where you want to save the files and click **Save**.

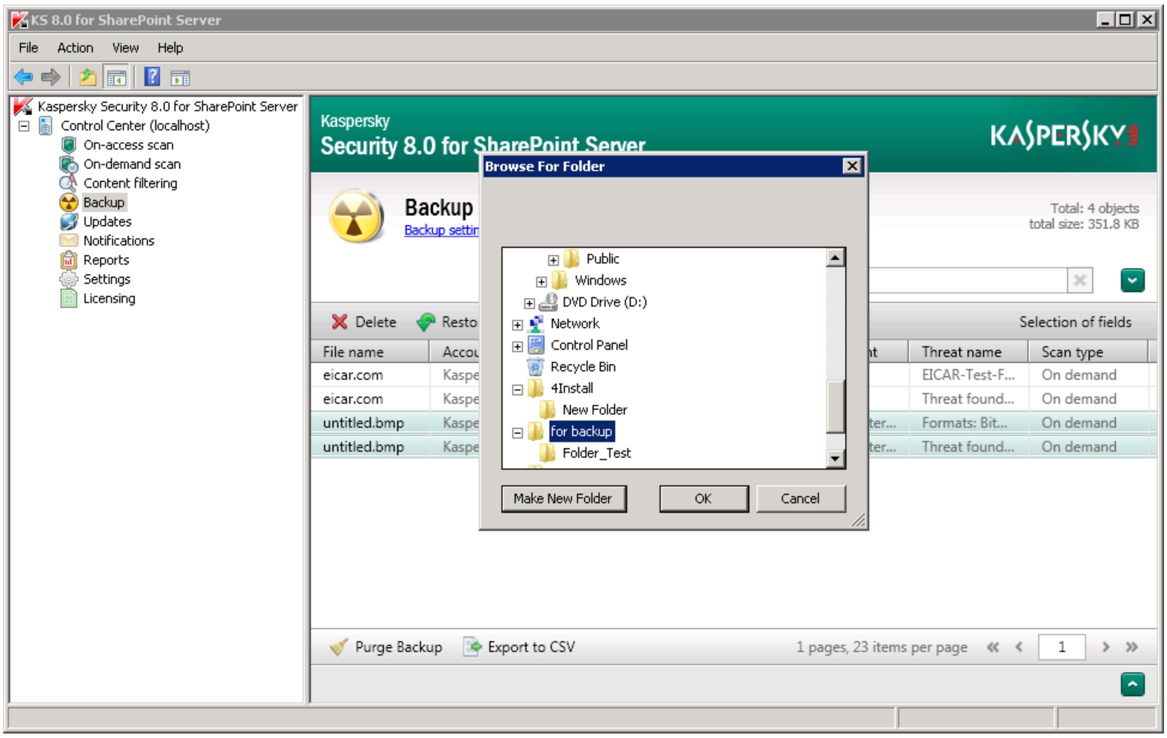


Figure 22: Saving a file from Backup

Selected files will be saved in the destination folder.

DELETING OBJECTS FROM BACKUP

➡ *To delete files from Backup:*

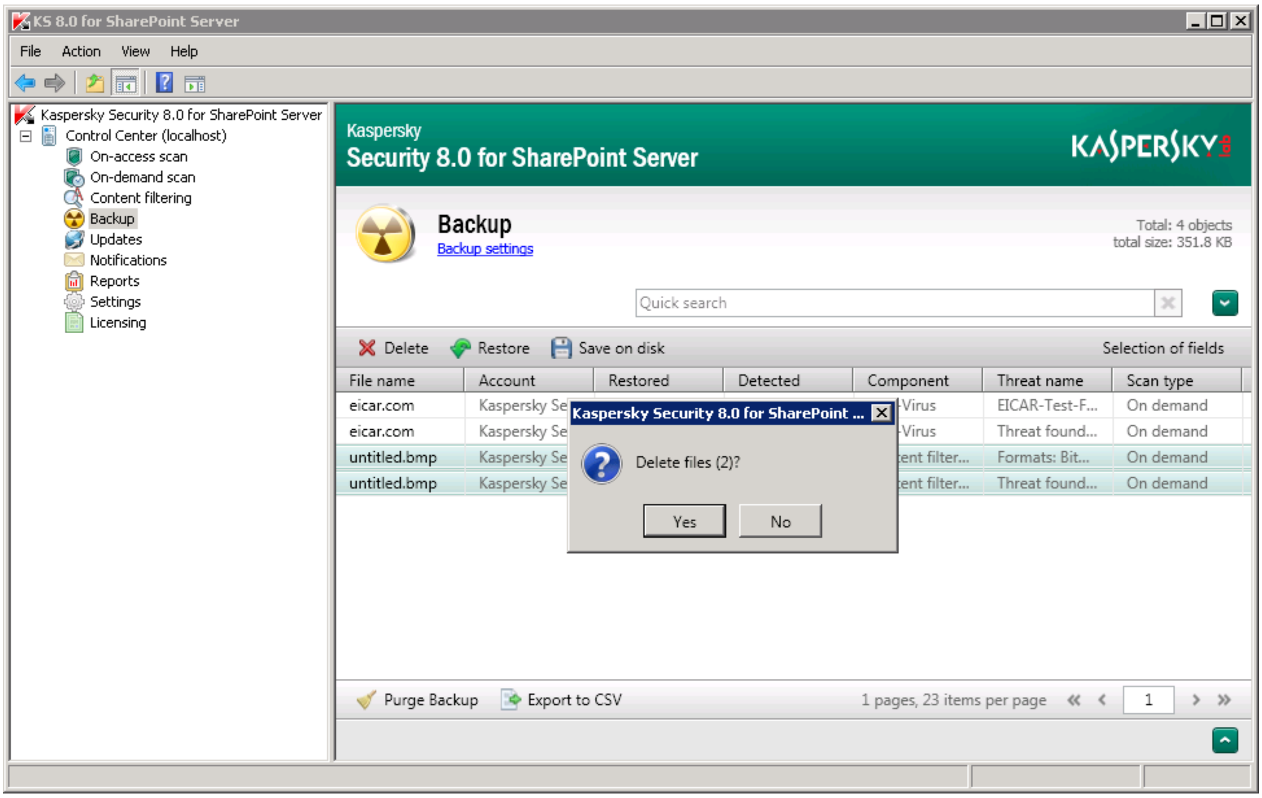
1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. Select in the list the files, which you want to delete. You may use quick search or extended filter to find the files.

Files will be deleted from Backup irreversibly. They cannot be restored.

3. Click **Delete** (see the figure below).



File name	Account	Restored	Detected	Component	Threat name	Scan type
eicar.com	Kaspersky Se			-Virus	EICAR-Test-F...	On demand
eicar.com	Kaspersky Se			-Virus	Threat found...	On demand
untitled.bmp	Kaspersky Se			tent filter...	Formats: Bit...	On demand
untitled.bmp	Kaspersky Se			tent filter...	Threat found...	On demand

Kaspersky Security 8.0 for SharePoint ...

Delete files (2)?

Yes No

Figure 23: Deleting a file from Backup

A warning dialog will appear.

4. Click **Yes**.

   Selected files will be deleted from Backup.

PURGING BACKUP

You can purge Backup by deleting all the objects inside it.

➧ *To purge the Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

2. In the details pane, click the **Purge Backup** button below the list of files stored in Backup.

   The application permanently deletes all files in Backup.

NOTIFICATIONS

This section describes notifications generated by the application, and configuration of their delivery to specified email addresses.

IN THIS SECTION:

ABOUT NOTIFICATIONS

Kaspersky Security supports the creation and delivery by email of notifications on the following events in the application:

- Events pertaining to the application licensing and license keys.
- Component incidents: detection of infected, probably infected, corrupted, or password-protected files and contain unwanted content during on-access or on-demand scanning;
- System events: events associated with Kaspersky Security databases, performance of on-demand scan tasks, and detection of inactive security servers of Kaspersky Security on SharePoint farm servers. Security Servers of Kaspersky Security are considered inactive if they have not accessed the SQL database storing configuration data for the application and Backup objects for more than 60 seconds.

CONFIGURING NOTIFICATIONS ABOUT KEY-RELATED EVENTS

➡ *To configure delivery of notifications about key-related events to specified email addresses:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Notifications** node.
2. In the **Licensing** configuration section specify the email addresses where the notifications should be sent:
   - **Notify the Administrator about events related to the keys**. Notifications will be sent to the administrator's email address specified in the **Settings** window (see section "**Configuring the application settings**" on page 94).
   - **Additional addresses**. Notifications will be sent to the email addresses specified in the field to the right.
3. To keep the changes, click the **Save** button in the upper part of the window.

CONFIGURING NOTIFICATIONS ABOUT SECURITY POLICY VIOLATIONS

➧ *To configure delivery of notifications about violations of security policies to specified email addresses:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Notifications** node.

2. In the **Security policy violation** section, select the check boxes corresponding to the events that should trigger notifications and the addresses to which they are to be sent:

   - **Administrator**. Notifications will be sent to the administrator's email address specified in the **Settings** window (see section "**Configuring the application settings**" on page 94).

   - **Author**. Notifications will be sent to the email address of the author of the document where scanning has revealed a security policy violation.

   - **User**. Notifications will be sent to the email address of the user who modified the document and the user who downloaded / uploaded it. The corresponding user address is stored in the SharePoint server settings.

   > In Microsoft SharePoint Server 2007, for technical reasons related to the server, notifications cannot be sent to the author of the document, the person who amended the document, or the user who uploaded or downloaded the document.

   - **Additionally**. Notifications will be sent to the email addresses specified in the **Additional addresses** field to the right.

3. To keep the changes, click the **Save** button in the upper part of the window.

CONFIGURING NOTIFICATIONS ABOUT SYSTEM EVENTS

➧ *To configure notifications about system events:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Notifications** node.

2. In the **System events** settings section, select check boxes opposite the types of system events about which you want to be notified:

   - **Database errors**. Information about application errors attributed to Kaspersky Security databases.

   - **On-demand scan task reports**. Reports with the details of on-demand tasks performed by the application.

   - **Inactive servers detected**. Information about Security Servers running Kaspersky Security, which are installed on SharePoint farm servers that did not contact the SQL server with the database for more than 60 seconds and/or that skip all files without scanning.

     Security Servers are considered *inactive* if they have not accessed the SQL database storing configuration data for the application and Backup objects for more than 60 seconds.

     A notification about an inactive Security Server of Kaspersky Security is sent within 60 seconds of a Security Server becoming inactive. Notifications are sent every 2 hours until the Security Server of Kaspersky Security queries the SQL server.

     If the connection with the SQL server is not reestablished within two hours, the Security Server switches to idle mode. A notification about the imminent switch to idle mode is sent 30 minutes after the connection to the SQL server was lost.

3. Select the check boxes opposite the email addresses to which notifications should be sent:

   - **Administrator**. Notifications are sent to the administrator's email address specified in the **Settings** window (see section "**Configuring the application settings**" on page 94).

   - **Additionally**. Notifications are sent to the email addresses specified in the **Additional addresses** on the right. Use a semicolon to separate addresses.

4. To save the changes, click the **Save** button in the upper part of the window.

REPORTS

This section describes operational reports, and contains guidelines on how to configure report content and report schedules.

IN THIS SECTION:

ABOUT REPORTS

Kaspersky Security generates Anti-Virus protection, Content filtering, and application activity reports that help to analyze information about the protection status of a SharePoint server or farm servers. Reports provide detailed information on the number of clean and infected files and the number of files disinfected and removed.

Report creation tasks in Kaspersky Security are used to create reports.

You can create new report creation tasks, delete or modify the existing ones and start selected tasks manually.

Reports can be generated automatically according to schedule or manually. You can view reports in the browser window or configure automatic delivery of reports to one or several email addresses. E-mailed reports are attached to a message.

You can create Quick reports about all events that occurred within a user-defined time interval.

The list of report generation tasks is displayed in the table in the results pane of the **Reports** node on the **Report creation tasks** tab. Report creation tasks that were or could not be run at the scheduled time are highlighted red.

The reasons for not running the tasks are displayed in the **Status** column:

- **Deleted: <Server name>**. Kaspersky Security Security Server has been deleted from the SharePoint server specified in the report creation task settings. You can specify a different SharePoint server in the task settings.

- **Task not executed**. The SharePoint server specified in the report creation task settings was not available at the time scheduled for the start of the task. The availability of the server needs to be checked. If necessary, you can generate a report manually by clicking the **Create report** button.

Reports open in the default browser. The following browsers are recommended for report viewing:

- Windows Internet Explorer 7.x (32-bit version).
- Windows Internet Explorer 7.x (64-bit version).
- Windows Internet Explorer 8.x (32-bit version).
- Windows Internet Explorer 8.x (64-bit version).
- Windows Internet Explorer 9.x (32-bit version).
- Windows Internet Explorer 9.x (64-bit version).
- Mozilla Firefox 3.6 or later.
- Google Chrome (last version).

CREATING A REPORT CREATION TASK

➧ *To create a new report creation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane of the **Reports** node on the **Report creation tasks** tab, click the **Create** button.

   The **Task settings** window can be used to configure report creation task settings.
3. Configure the report generation settings in the **Task settings** window, and click **OK**.

   Created task will be added to the list of tasks in the details pane. If necessary, you can edit the task settings (see section "Configuring a report creation task" on page 88).

STARTING A REPORT CREATION TASK

➧ *To start a report creation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane of the **Reports** node on the **Report creation tasks** tab, select the required report creation task from the list.
3. Click the **Create report** button.

CONFIGURING A REPORT CREATION TASK

➧ *To configure a report creation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane of the **Reports** node on the **Report creation tasks** tab, select the task whose settings you want to change, and click the **Change** button.

The **Task settings** window opens.

3. In the **Task settings** window, configure the following settings:

   - Edit the **Task name** in the corresponding field.
   - Select the **Run on schedule** check box if you want the application to generate the report according to the specified schedule, and choose from the drop-down list the server where the task will run. In the **Schedule** section, configure the task startup schedule:

     - **Every N days**. The report will be created at the defined time after the specified number of days. The report contains data for the last N days (collected from 0:00 of the first day to 0:00 of the report creation day).
     - **Weekly**. The report will be created at the defined time on the specified day of the week. The report contains data for the last 7 days (from 0:00 of the previous specified day of the week to 0:00 of the report creation day, for example, from Monday to Monday).
     - **Monthly**. The report will be created at the defined time on the specified day of the month. The report contains data for the last month (collected from 0:00 of the first date of the previous month to 0:00 of the first day of month when the report is created).

     > The report generation schedule uses the time of the SharePoint server where the task is started.

   - If you want the application to send the reports to the administrator's address specified in the **Notifications**, window, select the **Send to the Administrator** check box.
   - If you want to have the reports sent to other email addresses, select the check box **Send to recipients** and specify the addresses in the corresponding field. If several addresses are defined, use a semicolon as a delimiter.

4. To save the changes and close the window, click **OK**.

DELETING A REPORT CREATION TASK

➧ *To delete a report creation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane of the **Reports** node on the **Report creation tasks** tab, select in the list the task that you want to delete, and click the **Delete** button.

DELETING STATISTICS

➧ *To delete statistics data:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane of the **Reports** node, open the **Report creation tasks** tab.
3. Click the **Clear statistics** button to clear all statistics used in creating reports.

VIEW THE READY REPORTS

➧ *To view a ready report:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. Select on the **Reports** tab the report, which you would like to view and click the **View** button.

   The report opens in the default browser.

The report contains the following information:

- **Report parameters**:
  - Date and time of report generation.
  - Name of the SharePoint server for which the report has been generated.
  - Reporting period covered by the report.
- **File management report**: Information on the number of files processed by Kaspersky Security:
  - **Files submitted for scanning in the reporting period**. Files submitted for scanning during the reporting period.
  - **Recognized as clean**. Number of files recognized as clean after being scanned by application components to which they were referred for scanning.
  - **Disinfected**. Number of files that have been successfully disinfected by the application.
  - **Deleted**. Number of files that have been deleted after scanning.
  - **Blocked**. Number of files that have been blocked during on-access scanning.
  - **Skipped (threat detection only)**. Number of files that have been skipped by the application after anti-virus scanning and content filtering according to the configured settings of on-demand and on-access scanning.
  - **Not processed**. Number of files that have not been scanned by at least one Kaspersky Security component.
- **Anti-Virus protection status report**:
  - Information on the number of files referred for virus scanning.
  - Status labels assigned by the application to files as a result of virus scanning:
    - **Uninfected**. Number of files that have been found to be free from threats during virus scanning.
    - **Infected**. The number of files with a code segment fully matching a code segment of a known application posing a threat.
    - **Potentially infected**. The number of files whose code contains a modified segment of code of a known application posing a threat, or files resembling such application in the way it they behave.
    - **Password-protected**. Number of password-protected archives.
    - **Corrupted**. Number of files that cannot be read by Kaspersky Security.
  - Information about skipped files:

        - **Excluded from scanning by the Administrator**. Number of files that have been skipped according to the virus scan exclusion settings.
        - **License problems**. The number of files that have not be scanned due to license errors (such as a missing key).
        - **Processing error**. Number of files that have been skipped due to errors during virus scanning.
    - Actions taken by the application on files found to contain threats.
        - **Disinfected**. Number of files disinfected after virus scanning.
        - **Deleted**. Number of files deleted after virus scanning.
        - **Blocked**. Number of files blocked after virus scanning.
        - **Skipped (threat detection only)**. Number of files that, although found to contain a threat during virus scanning, have been skipped because the **Skip** action has been specified for them in the scan settings.

- **Content filtering report**:
    - Information on the number of files referred for Content filtering.
    - Status labels assigned by the application to files as a result of Content filtering:
        - **Allowed**. The number of files that have been found to be free from violations of Content filtering policies.
        - **Forbidden format**. The number of times that the Content filtering component detected prohibited file formats specified in the Content filtering settings.
        - **Forbidden mask**. The number of times that the Content filtering component detected file names that match masks specified in the Content filtering settings.
        - **Forbidden content**. The number of times that the Content filtering component detected words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the Content filtering settings.

> If one and the same file causes multiple detections by the Content filtering component in a number of categories, each detection is recorded under the corresponding category.

    - Information about skipped files:
        - **Excluded from scanning by the Administrator**. The number of files that have been skipped according to the Content filtering exclusion settings.
        - **Text extraction errors**. Number of files whose contents have not been scanned by the application due to text extraction errors. Such errors may be caused by errors in the corresponding filter of IFilter Utility or a stopped Kaspersky Text Extracting Service.
        - **License problems**. The number of files whose content has not been scanned by the applications to due license violations, such as a missing or blacklisted key.
        - **Text filter is not available**. Number of files whose contents have not been scanned by the application because the corresponding filter of IFilter Utility is disabled or not installed.
        - **Processing error**. The number of files that have been skipped due to other errors occurring during content filtering.
    - Actions taken by the application on files found to contain unwanted content.

        - **Deleted**. The number of files for which the action is set to **Delete** in Content filtering settings.
        - **Blocked**. The number of files for which the action is set to **Block** in Content filtering settings.
        - **Skipped (threat detection only)**. The number of files for which the action is set to **Skip** in Content filtering settings.

- **SharePoint web objects scan report**:
    - The number of SharePoint web objects referred for Content filtering in the reporting period.
    - Actions taken by the application on SharePoint web objects based on the results of content filtering:
        - **Recognized as clean**. The number of SharePoint web objects that have been found to be free from violations of Content filtering policies.
        - **Blocked**. The number of SharePoint web objects that have been blocked based on the results of content filtering.
        - **Skipped (threat detection only)**. Number of SharePoint web objects that, although found to contain unwanted content, have not been blocked because the **Skip** action has been specified for them in the scan settings.
        - **Phishing**. Number of SharePoint web objects found to contain phishing URLs.

    During on-demand scanning, the application skips all web objects containing unwanted content regardless of the action configured for the Content filtering component.

    - Information on skipped SharePoint web objects:
        - **Licensing errors**. The number of SharePoint web objects that have not be scanned due to license errors (such as a missing key).
        - **Processing error**. The number of SharePoint web objects that have been skipped due to errors occurring during content filtering.

CREATING QUICK REPORTS

To generate a Quick report:

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the details pane, click on the **Report**s tab the **Quick report** button.
3. Select in the displayed **Quick report settings** window the time period, which the report should cover:
    - **Daily**. The report will cover the 24 hours specified in the date field.
    - **For period**. The report will cover the selected time period.
4. Click **OK**.

DELIVERY OF REPORTS VIA EMAIL

➧ *To configure delivery of generated reports by email:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.

2. In the details pane, go to the **Report creation tasks** tab, select the task in the list and click the **Change** button.

3. In the displayed **Task settings** window select the check boxes corresponding to the appropriate recipients:

   - **Send to the Administrator**. The report will be sent to the administrator's email address specified in the **Settings** window (see section "**Configuring the application settings**" on page 94).

   - **Send to recipients**. The report will be sent to the email addresses specified in the field to the right. If several addresses are defined, use the semicolon as a delimiter.

CONFIGURING THE APPLICATION SETTINGS

This section describes configuration of the following application settings:

- Email sending settings
- Logging settings
- Backup purging settings

IN THIS SECTION:

ABOUT PARTICIPATION IN KASPERSKY SECURITY NETWORK

To protect SharePoint servers more effectively, Kaspersky Security uses data that is collected from users around the globe. *Kaspersky Security Network* is designed to collect such data.

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, online resources, and software. Using data from Kaspersky Security Network ensures a faster response time for Kaspersky Security when encountering new types of threats and improves performance of some protection components.

User participation in Kaspersky Security Network helps Kaspersky Lab to gather real-time information about the types and sources of new threats and develop methods of neutralizing them. Participation in Kaspersky Security Network also lets you access reputation statistics for applications and websites.

You can use Kaspersky Security Network if the application license has not expired and the key has not been blacklisted.

Kaspersky Security Network can be used as a vehicle for sending application performance statistics to Kaspersky Lab virus analysts. This information makes it possible to keep track of threats in real time.

When you participate in Kaspersky Security Network, certain statistics are collected while Kaspersky Endpoint Security is running and are automatically sent to Kaspersky Lab (see section "About data submission" on page 27). Also, additional checking at Kaspersky Lab may require sending files (or parts of files) that are imposed to an increased risk of being exploited by intruders to do harm to the user's computer or data.

Participation in Kaspersky Security Network is voluntary. To start using Kaspersky Security Network, you have to accept the terms of a special agreement – the Kaspersky Security Network Statement. You can also opt out of participating in Kaspersky Security Network at any time (see section "Configuring KSN protection settings" on page 95). No personal data of the user is collected, processed, or stored by the Kaspersky Security Network service. The types of data that Kaspersky Security sends to Kaspersky Security Network are also described in the Kaspersky Security Network Statement.

KSN PROTECTION SETTINGS

➧ *To configure the KSN protection settings:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. In the **KSN Protection Settings** section, select the **I accept the KSN agreement and I want to use KSN** if you accept the terms of the Kaspersky Security Network Statement. You can view its text by clicking the **Full KSN agreement** button.

   When the Kaspersky Security upgrade process is started, the **I accept the KSN agreement and I want to use KSN** check box is automatically cleared.
3. To use the KSN cloud service for protection of SharePoint web objects, select the **Use Kaspersky Security Network** check box.

   Information from Kaspersky Security Network is used during anti-virus scanning of web objects for phishing threats.
4. Specify the KSN request wait time. The default wait time for a response from the cloud is 10 seconds.
5. Select the **Use proxy to access KSN** check box to exchange information with the KSN service via a proxy server.

   To configure the proxy server settings, select the **Updates** node in the tree of Administration Console corresponding to the SharePoint server. The proxy server settings are found in the **Connection settings** section. The way to configure the proxy server settings is described in the automatic database update configuration instructions (see page 34).
6. Click the **Save** button.

ENABLING AND DISABLING ZETA SHIELD TECHNOLOGY

ZETA Shield is a technology that recognizes vulnerabilities and malware against which no protection is yet available. ZETA Shield helps to effectively repel targeted attacks against the local area network and supplements the anti-virus databases.

➧ *To enable / disable ZETA Shield that protects servers against vulnerabilities:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. In the **Protection against vulnerabilities** section, do one of the following:
   - Select the **Use ZETA Shield technology** check box if you want the application to scan files for malicious code that exploits system vulnerabilities.
   - Clear the **Use ZETA Shield technology** check box if you do not want the application to scan files for malicious code that exploits system vulnerabilities.

3. To keep the changes, click the **Save** button in the upper part of the window.

By default, ZETA Shield is enabled to protect SharePoint servers if the **Enable protection** check box was selected during installation of the application.

CONFIGURING EMAIL NOTIFICATION DELIVERY SETTINGS

➡ *To configure the notification delivery settings:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node. Notification delivery settings are available in the section **SMTP server configuration for delivery of notifications.**
2. Specify in the **Administrator's address(es)** field the email address of the Kaspersky Security administrator.
3. Enter in the **Send as** field the name that will be substituted as the email sender.

   By default, the field value defined in the SharePoint server settings is used. If the field value is not defined in the **Settings** node and in the SharePoint settings, the reports and notifications are not sent.
4. Select the appropriate SMTP configuration:
   - If you want to use SMTP settings defined on the SharePoint server, select the option to **Use SMTP settings of the SharePoint server**.
   - If you want to use other SMTP settings, select the option to **Use custom SMTP server settings** and fill in the **SMTP server address**, **Account** and **Password** fields. If NTLM authentication has to be used, select the **Use NTLM authentication** check box.
5. To make sure that the configuration is correct, click the **Send message using specified settings** button.

   A test message will be sent to the specified email address of the administrator.
6. To keep the changes, click the **Save** button in the upper part of the application window.

CONFIGURING THE LOGGING SETTINGS

You can configure the diagnostics settings: the level of detail and size limit applicable to the log file storing application activity information.

➡ *To restrict the size of log files:*

1. Select and open in the console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. In the **Diagnostics** configuration section, specify the maximum log file size (MB) in the **Maximum file size** text box. By default, the maximum size of log files is 100 MB.

➡ *To configure the amount of details in the log file:*

1. Select and open in the console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. Use the **Detail level** drop-down list to define the amount of details in the log file:
   - **Minimum**. Log file will contain only basic information about the application activity: the results of scanning, database updates and key addition.

- **Other**. Log file will contain information about the activity of components selected in the **Diagnostics settings** window that opens after clicking the **Settings** button to the right of the drop-down list.

3. To keep the changes, click the **Save** button in the upper part of the window.

When a log is kept with a high level of detail, the URLs scanned for phishing threats are recorded in the log.

CONFIGURING AUTOMATIC BACKUP PURGING

➧ *To configure automatic Backup purging:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.

2. Select the check box **Purge Backup automatically if its size exceeds ... MB**.

3. Enter in the entry field maximum Backup size (MB).

   Supported parameter values are 1 –1048576 MB. If there is a storage size restriction and the addition of a new file exceeds this restriction, the application frees up the necessary space by deleting the oldest files. The default size of Backup is 3686 MB.

4. To keep the changes, click the **Save** button in the upper part of the application window.

FAILSAFE SUPPORT FOR SQL DATABASES

Kaspersky Security supports the following failsafe technologies for SQL databases:

- Failover Clustering. Supported automatically.

- Database Mirroring. Supported automatically.

- Log Shipping. When the database used by the application (primary database) fails, the server hosting the restored database needs to be specified manually in order to switch to this database.

Using Database Mirroring technology

If your SQL server is configured to use the Database Mirroring failover support technology, the application automatically switches from the primary database that has failed to a mirror database, and then back to the primary database after it has been restored.

If the SQL server is running in **High Performance** Mode or **High Safety Mode Without Automatic Failover** for Database Mirroring, manual switchover to Database Mirroring is required by means of the SQL server if the main database used by Kaspersky Security fails.

Using Log Shipping technology

If your SQL server is configured to use the Log Shipping failover support technology, you can switch to using a restored database when the primary database fails. This switch is performed manually.

➧ *To switch to the restored database when using Log Shipping technology:*

1. In the folder <Application installation folder>\Configuration, open the file BackendDatabaseConfiguration.config in a text editor.

2. Specify the name of the SQL server (indicating the SQL server instance) that hosts the failover partner in the line <SqlServerName>SQL server name\instance</SqlServerName>.

3. Save the file.

   The changes will take effect within one minute.

If Kaspersky Security is installed on a SharePoint farm, the corresponding changes to the file BackendDatabaseConfiguration.config need to be made on all SharePoint farm servers.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION:

HOW TO OBTAIN TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see section "Sources of information about the application" on page 10), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact Technical Support specialists through a request form.

Technical support is only available to users who purchased a license for the application. No technical support is available to users of trial versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists at Russian-speaking or international Technical Support (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules). This will allow our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

Kaspersky CompanyAccount is a web service for sending requests relating to corporate products to Kaspersky Lab and tracking the progress made in processing them.

To access Kaspersky CompanyAccount, register on the registration page https://support.kaspersky.com/companyaccount/register To log into Kaspersky CompanyAccount, enter the Client ID (identification number of the client) and password generated by the Kaspersky Lab server upon registration.

You can do the following in Kaspersky CompanyAccount:

- Contact Technical Support and the Virus Lab.
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

An email request to the Technical Support Service

You can send an online request to Technical Support in English, Russian, German, French, or Spanish.

In the fields of the online request form, specify the following data:

- Request type
- Application name and version number
- Request description
- Customer ID and password
- email address

A Technical Support Service representative sends an answer to your question to your Kaspersky Account and to the email address that you specified in your online request.

Online request to the Virus Lab

Some requests must be sent to the Virus Lab instead of Technical Support.

You can send requests to the Virus Lab in the following cases:

- If you suspect that a file or website contains a virus, but Kaspersky Security does not detect any threat. Virus Lab specialists analyze the file or URL that you send. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when Kaspersky Lab anti-virus applications are updated;
- If Kaspersky Security detects a virus in a file or website, but you are certain that this file or website is safe.

You can also send requests to the Virus Lab from the request form page (http://support.kaspersky.com/virlab/helpdesk.html) without registering My Kaspersky Account.

USING INFO COLLECTOR

When you inform Technical Support of the problem, you may be asked to create an archive with data on the operation of the application using the SharePoint.InfoCollector.exe utility, and to send it to Technical Support.

You can read a description of Info Collector and download the tool at: http://support.kaspersky.com/faq/?qid=208642392.

GLOSSARY

A

Activating the application

Switching the application into full-function mode. Application activation is performed by the user during or after the application installation. You should have a key file to activate the application.

Active key

Key that is used at the moment to work with the application.

Additional key

Key that verifies the use of the application but is not used at the moment.

Administration Console

Kaspersky Security application component. Provides the user interface for managing the application's administrative services and enables configuration of the application and management of the server component. The management module is implemented as an extension of the Microsoft Management Console (MMC).

B

Backup

Special Backup of objects created prior to their first disinfection or removal.

Black list of key files

Database that contains information about the key files blocked by Kaspersky Lab. The black list file content is updated along with the product databases.

D

Database update

A function performed by a Kaspersky Lab application that enables it to keep computer protection up-to-date. During the update, an application downloads updates for its databases and modules from Kaspersky Lab's update servers and automatically installs and applies them.

Databases

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the databases. Records in the databases allow detection of malicious code in the objects being scanned. Databases are compiled by Kaspersky Lab specialists and are updated hourly.

Deleting an object

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfected.

Disinfection

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

I

INFECTED OBJECT

An object a segment of whose code fully matches a code segment of a known threat. Kaspersky Lab does not recommend using such objects.

K

KASPERSKY COMPANYACCOUNT

A web service for sending requests to Kaspersky Lab and tracking the progress made in processing them by the Kaspersky Lab experts.

KASPERSKY LAB UPDATE SERVERS

HTTP and FTP servers of Kaspersky Lab from which Kaspersky Lab applications download database and component updates.

KASPERSKY SECURITY NETWORK (KSN)

Infrastructure of online services providing access to the current knowledge base of Kaspersky Lab describing the reputation of files, web sites and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Lab apps to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

KEY FILE

A file with the .key extension that makes it possible to use a Kaspersky Lab application on the terms of a trial or commercial license. You have to specify the path to the key file after the application has been installed. You may use the application only when you have a key file.

L

LICENSE CERTIFICATE

A document that Kaspersky Lab transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

LICENSE TERM

License term is a time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

O

ON-ACCESS SCAN

A mode of a Kaspersky Lab application whereby files are scanned automatically on being uploaded to the server or downloaded from the server.

ON-DEMAND SCAN

Kaspersky Lab's program operation mode initiated by the user and designed to scan and check any resident files.

P

PHISHING

A kind of Internet fraud, when email messages are sent with the purpose of stealing confidential information. As a rule, this information relates to financial data.

POTENTIALLY INFECTED OBJECT

An object whose code contains a modified segment of code of a known threat, or an object resembling a threat in the way it behaves.

S

SHAREPOINT SERVER STRUCTURE

A tree of nodes that makes it possible to manage the content of a SharePoint server. In nodes, you can select elements and specify the actions to take on them.

SKIPPING OF AN OBJECT

Processing method in which an object is allowed to pass to the user unchanged. If event logging is enabled for this event type, information about the object detected will be logged in the report.

U

UNWANTED CONTENT

Information that is unsuitable for various groups of users. Unwanted content includes websites and messages that propagate violence, incite acts of terror, contain child pornography or profanity.

V

VIRUS

A program that infects other ones by adding its code to them in order to gain control when infected files are run. This simple definition allows exposing the main action performed by any virus – infection.

Z

ZETA SHIELD

A technology that recognizes vulnerabilities and malware against which no protection is yet available. ZETA Shield helps to effectively repel targeted attacks against the local area network and supplements the anti-virus databases.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*, *and the Anti-Spam database – every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com/
Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archives) http://support.kaspersky.com/virlab/helpdesk.html?LANG=en (for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ON THE THIRD-PARTY CODE

Information about third-party code can be found in the file named legal_notices.txt and stored in the application installation folder.

TRADEMARK NOTICES

The registered trademarks and service marks are the property of their owners.

Google Chrome is a trademark owned by Google, Inc.

Internet Explorer, Microsoft, SharePoint, Windows, Windows Server, and Windows Vista are trademarks of Microsoft Corporation registered in the USA and elsewhere.

Firefox, Mozilla is trademark of the Mozilla Foundation.

INDEX